Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Eidgenössische Finanzverwaltung EFV
Rechtsdienst
Risikomanagement und Versicherungspolitik

Handbuch zum Risikomanagement Bund

Version vom 10.09.2015

Änderungskontrolle

Wann	Wer	Beschreibung
21.11.2011	rch	Erstversion (Prüfung durch Kessler und AON)
24.05.2013	rch	Einfügen Risikoaggregation von Querschnittsrisiken (inkl. Anhang «Factsheets Querschnittsrisiken Bund»
24.05.2013	rch	Einfügen Prozess Risiko-Update
10.09.2015	mlu	Überarbeitung Schnittstellen, IKT-Risiken, Definitionen und redaktionelle Korrekturen

Inhaltsverzeichnis

Abbildungsverzeichnis **6**

Abkürzungsverzeichnis **7**

0 Zweck dieses Dokuments **8**

1 Grundlagen des Risikomanagements des Bundes **8**

1.1 Risikopolitik **8**
1.1.1 Ziele 8
1.1.2 Nutzen 9

1.2 Risikostrategie und Risikokultur **9**
1.2.1 Risikostrategie Bund 9
1.2.2 Risikokultur 10

1.3 Geltungsbereich und Risikodefinition **10**
1.4 Umgang mit als GEHEIM klassifizierten Informationen **10**

2 Organisation des Risikomanagements Bund **11**

2.1 Aufbau **11**
2.2 Funktionen und Verantwortlichkeiten **11**
2.3 Einbettung des Risikomanagements in die Führungsprozesse der Bundesverwaltung **12**
2.3.1 Strategie- und Planungsprozesse 12
2.3.2 Weitere Prozesse 13

3 Risikomanagementprozess **13**

3.1 Prozessabläufe und Informationsflüsse in der Bundesverwaltung **14**
3.1.1 Jährliches Risikoreporting 15
3.1.2 Risiko-Update 15
3.1.3 Informationsflüsse im Risikomanagement Bund 16

3.2 Identifikation **17**
3.2.1 Ausgangspunkte und Abgrenzung 17
3.2.2 Vorgehen 18

3.3 Analyse und Bewertung **20**
3.3.1 Allgemeines zum Erfassen von Risiken 20
3.3.2 Methoden zur Analyse und Bewertung von Risiken 20
3.3.3 Schadensverteilung eines Risikos 21
3.3.4 Bewertung der Auswirkungen 22
3.3.5 Qualitative oder quantitative Bewertung 23
3.3.6 Bewertung der Eintrittswahrscheinlichkeit 24
3.3.7 Wechselwirkungen zwischen Risiken 24

3.4 Beurteilung **25**
3.5 Bewältigung **26**
3.5.1 Bewältigungsoptionen 26
3.5.2 Definition, Auswahl und Umsetzung von Massnahmen 27

3.6 Überwachung **28**
3.6.1 Risiko-Überwachung 28
3.6.2 Massnahmen-Überwachung 28

4 Reporting **28**

4.1 Inhalt des Risikoreportings **29**

4.2 Reporting-Grundsätze 29
4.3 Aggregation von Querschnittsrisiken 29
4.3.1 Aggregationsentscheid 30
4.3.2 Zuständigkeit für die Aggregation 30
4.3.3 Klärung der Verantwortlichkeiten 31
4.3.4 Reporting 31
4.3.5 Informationsaustausch 31
4.4 Auswahl von Risiken 32
4.5 Wechselwirkungen 33
4.5.1 Organisatorischer Umgang mit Wechselwirkungen 33
4.5.2 Abbildung von Wechselwirkungen 33
5 Kommunikation 34
5.1 Interne Kommunikation und Schulungen 34
5.1.1 Schulungen 35
5.1.1.1 Kurs «Risiken verstehen und bewältigen» 35
5.1.1.2 Schulung R2C 35
5.1.1.3 Ausbildungskurs für Kader (Risikoeigner) 35
5.1.2 Veranstaltungen 36
5.1.3 Interne Informationskanäle 36
5.1.3.1 Intranetbereich Risikomanagement 36
5.1.3.2 Newsletter Risikomanagement 36
5.2 Externe Kommunikation 36
5.2.1 Geschäftsbericht 36
5.2.2 Staatsrechnung und Voranschlag (Budget) 37
5.2.3 Stellungnahme des Bundesrates zu parlamentarischen Berichten bezüglich Risikomanagement 37
5.3 Klassifizierung, Öffentlichkeitsprinzip und Archivierung 38
5.3.1 Klassifizierung von Informationen im Risikomanagement 38
5.3.2 Öffentlichkeitsprinzip 38
5.3.3 Archivierung 38
6 Schnittstellen 39
6.1 Internes Kontrollsystem (IKS) 39
6.2 Notfall- und Krisenmanagement 40
6.3 Kontinuitätsmanagement 43
6.4 Perspektivstab 44
6.5 Corporate Governance 44
6.6 Versicherungsmanagement 46
6.7 Informatiksteuerungsorgan des Bundes 46
6.8 Eidgenössische Finanzkontrolle (EFK) 47
6.9 Weitere Schnittstellen 48
7 Verbesserung des Risikomanagements Bund 49
7.1 Leistungsbewertung 49
7.2 Audit / Review 49
7.3 Zertifizierung 50
Anhang 1: Begriffsdefinitionen 51
Anhang 2: Risikoerfassungsbogen 56
Anhang 3: Strukturierung von Risiken 57
Anhang 4: Pflichtenhefte für Risikomanager und Risikocoaches 59

Anhang 5: Beispiel einer Einsichtsverweigerung in das Risikomanagement Bund (konkret: in die Risikodatenbank R2C) 61

Anhang 6: Schnittstelle «Risikomanagement – Rechnungslegung» im Bund ... 63

Anhang 7: Organisationen ausserhalb der Bundesverwaltung 64

Anhang 8: Projekte mit Bezug zum Risikomanagement 69

Anhang 9: Stolpersteine im Risikomanagement 70

Anhang 10: Factsheets «Querschnittsrisiken Bund» 73

Abbildungsverzeichnis

Abbildung 1: Organisation Risikomanagement Bund 11
Abbildung 2: Integriertes Risikomanagement 12
Abbildung 3: Vernetzung von Führungsprozessen in der Bundesverwaltung 13
Abbildung 4: Risikomanagementprozess nach gängigen Normen 14
Abbildung 5: Prozessabläufe im Risikomanagement Bund 14
Abbildung 6: Prozessablauf des jährlichen Risikoreportings in der Bundesverwaltung 15
Abbildung 7: Informationsflüsse 16
Abbildung 8: Risikoidentifikation 19
Abbildung 9: Schadensverteilung eines Risikos 22
Abbildung 10: Gesamtbewertung der Auswirkung 23
Abbildung 11: Beispiel Risikotoleranzstufen 25
Abbildung 12: Auswahl von Top-Risiken 32
Abbildung 13: Auswahl von Risiken in der Bundesverwaltung 33
Abbildung 14: Schnittstellen zum Risikomanagement (nicht abschliessend) 39
Abbildung 15: IKS und Risikomanagement 40
Abbildung 16: Schnittstelle Risikomanagement und Krisenmanagement 41
Abbildung 17: Überblick Krisenmanagement-Organisationen 42

Aus Gründen der Lesbarkeit wird in diesem Handbuch für die Funktionsbezeichnungen die männliche Form verwendet. Selbstverständlich gelten die Ausdrücke für beiderlei Geschlecht.

Abkürzungsverzeichnis

BAG	Bundesamt für Gesundheit
BCM	Business Continuity Management (Kontinuitätsmanagement)
BGA	Bundesgesetz über die Archivierung (SR *152.1*)
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (SR *152.3*)
BK	Bundeskanzlei
BöB	Bundesgesetz über das öffentliche Beschaffungswesen (SR *172.056.1*)
BR	Bundesrat
BWL	Bundesamt für wirtschaftliche Landesversorgung
CG	Corporate Governance
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDI	Eidgenössisches Departement des Innern
EDV	Elektronische Datenverarbeitung
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EFD	Eidgenössisches Finanzdepartement
EFV	Eidgenössische Finanzverwaltung
EO ABCN	Einsatzorganisation ABCN (Atomar, Biologisch, Chemisch, Naturereignisse)
FHG	Finanzhaushaltgesetz (SR *611.0*)
FHV	Finanzhaushaltverordnung (SR *611.01*)
GPK	Geschäftsprüfungskommissionen
GSK	Generalsekretärenkonferenz
IKS	Internes Kontrollsystem
ISchV	Informationsschutzverordnung (SR *510.411*)
ISDS	Informationssicherheit- und Datenschutzkonzept
ISO	International Organization for Standardization
IT	Information Technology
KOVE	Koordination Verkehrswesen im Ereignisfall
NAZ	Nationale Alarmzentrale
NDB	Nachrichtendienst des Bundes
OE	Organisationseinheit
ONR	Regelwerk des Österreichischen Normungsinstituts
PC	Personal Computer
RC	Risikocoach
RVOG	Regierungs- und Verwaltungsorganisationsgesetz (SR *172.010*)
R2C	Risk-to-Chance (Risikomanagement-Software)
SANKO	Sanitätsdienstliches Koordinationsgremium
SiA	Sicherheitsausschuss Schweiz
SOGE	Sonderstab Geiselnahme und Erpressung
SONIA	Sonderstab Informationssicherung
SOPA	Sonderstab Pandemie
SVS	Sicherheitsverbund Schweiz
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VE	Verwaltungseinheit
VG	Verantwortlichkeitsgesetz (SR *170.32*)
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung

0 Zweck dieses Dokuments

Das vorliegende Handbuch zum Risikomanagement des Bundes dient als Ergänzung bzw. Erläuterung der Richtlinien über das Risikomanagement Bund[1]. Es wird von der EFV nach Anhörung der Risikomanager der Departemente und der Bundeskanzlei (BK) herausgegeben.

Das Handbuch lehnt sich an die gängigen Normenwerke[2] an. Die im Risikomanagement Bund verwendeten Begriffe werden in Anhang 1 näher erläutert bzw. definiert. Das Handbuch unterstützt die im Risikomanagement tätigen Personen (insbesondere Risikomanager, Risikocoaches, Risikoeigner) bei der Erfüllung ihrer Aufgaben und dient den Führungskräften und Mitarbeitenden der Bundesverwaltung als Nachschlagewerk für Fragen im Zusammenhang mit dem Risikomanagement des Bundes.

In grau unterlegten Kästchen werden einerseits verbindliche Vorgaben und andererseits Empfehlungen an die Risikomanager und Risikocoaches aufgeführt. Die Vorgaben sind notwendig, um eine einheitliche Umsetzung des Risikomanagements und eine konsolidierte Berichterstattung auf Stufe Bundesrat zu ermöglichen.

Das vorliegende Handbuch regelt die wichtigsten Elemente des Risikomanagement-Systems des Bundes, insbesondere:

- die Risikomanagement-Politik (vgl. Ziff. 1);
- die Organisation des Risikomanagements Bund (vgl. Ziff. 2);
- die Funktionsbeschreibungen im Risikomanagement Bund (vgl. Ziff. 2.2);
- den Risikomanagementprozess (vgl. Ziff. 3);
- die Risikoberichterstattung (vgl. Ziff. 4);
- die Kommunikation innerhalb des Risikomanagements (vgl. Ziff. 5);
- Schnittstellen zwischen dem Risikomanagement und anderen Prozessen und Organisationen (vgl. Ziff. 6).

Das Handbuch wird aufgrund aktueller Bedürfnisse periodisch angepasst und weiterentwickelt. Die Departemente und die BK können entsprechende Anträge stellen.

1 Grundlagen des Risikomanagements des Bundes

1.1 Risikopolitik

Die Risikopolitik des Bundes legt die Ziele des Risikomanagement Bund fest und zeigt dessen Nutzen auf.

1.1.1 Ziele

Das Risikomanagement ist ein Führungsinstrument auf den Stufen Bundesrat (BR), Departement / BK und Verwaltungseinheiten (VE). Es schafft Transparenz über die aktuelle Risikosituation des Bundes und der einzelnen Organisationseinheiten (OE) und ermöglicht es, rechtzeitig die erforderlichen Massnahmen zur Vermeidung oder Verminderung der Risiken zu

[1] Diese Richtlinien wurden von der EFV gestützt auf Ziff. 6 Abs. 1 der Weisungen des Bundesrates vom 24. September 2010 über die Risikopolitik des Bundes erlassen (vgl. BBl *2010* 6549; hiernach: Weisungen)
[2] Konkret: ISO 31000, ONR 49000 ff.

treffen. Das Risikomanagement Bund soll:

- Die Erfüllung der verfassungs- und gesetzmässigen Aufgaben der Bundesverwaltung und die Erreichung der Ziele des Bundes unterstützen;
- Dem Bundesrat und der Bundesverwaltung ermöglichen, ihre Entscheide unter Berücksichtigung möglicher künftiger Ereignisse und Entwicklungen zu fällen, indem wesentliche negative Auswirkungen auf die Erfüllung der Aufgaben und die Erreichung der Ziele frühzeitig erkannt und analysiert werden;
- Seine eigene Wirksamkeit laufend überprüfen und die stetige Weiterentwicklung und Verbesserung sicherstellen.

Ausserdem soll die Sicherheit der Vertreter des Bundes gewährleistet, das Vermögen und die Reputation des Bundes geschützt und die verfügbaren Mittel wirksam und wirtschaftlich eingesetzt werden.[3]

1.1.2 Nutzen

Nach einheitlichen Kriterien umgesetzt, ist das Risikomanagement ein Instrument mit vielfältigem Nutzen für den Bund[4]:

- es trägt zu einer vorausschauenden Erfüllung der Bundesaufgaben bei und fördert eine proaktive Führung;
- es trägt zur Funktionsfähigkeit von Regierung und Verwaltung bei;
- es erhöht die Transparenz und die Übersicht über die Risikosituation und erleichtert damit die Entscheidfindung auf allen Führungsebenen;
- es ermöglicht eine wirksame und wirtschaftliche Zuteilung der erforderlichen Ressourcen für die Minimierung von Risiken;
- es trägt bei, das Vertrauen der verschiedenen Anspruchsgruppen (Bundesversammlung, Bevölkerung usw.) in die Bundesverwaltung und den Bundesrat zu erhöhen;
- es sensibilisiert Mitarbeitende in der Bundesverwaltung im Umgang mit den Risiken in ihrem Bereich.

1.2 Risikostrategie und Risikokultur

1.2.1 Risikostrategie Bund

Risiken im Zusammenhang mit der Erfüllung gesetzlicher Aufgaben lassen sich nicht immer vermeiden. Der Bund ist bereit, Risiken kontrolliert und bewusst einzugehen, sofern dies für die Zielerreichung bzw. die Aufgabenerfüllung unvermeidbar ist. Getreu dem Grundsatz des haushälterischen Umgangs mit Mitteln des Bundes sollen die mit der Erfüllung der Bundesaufgaben einhergehenden Risiken möglichst gering gehalten werden. Der Entscheid betreffend die Umsetzung risikominimierender Massnahmen erfolgt gestützt auf Kosten- / Nutzenüberlegungen (inkl. einer Rechtsgüterabwägung[5]).

Der Bund trägt das Risiko für Schäden an seinen Vermögenswerten und für die haftpflichtrechtlichen Folgen seiner Tätigkeit grundsätzlich selbst[6] (Grundsatz der Eigenversicherung). Einer finanziellen Risikoüberwälzung (z.B. mittels Abschluss eines Versicherungsvertrags, Derivate usw.) stimmt die EFV nur in besonderen Fällen zu[7].

---

[3] Ziff. 3 Abs. 1 der Weisungen
[4] Vgl. Ziff. 3 der Weisungen
[5] z.B.: Menschenwürde, körperliche Unversehrtheit (Leib und Leben), Eigentum usw.
[6] Art. 50 Abs. 2 FHV
[7] Vgl. Weisungen der EFV vom 02.02.2009 über die Risikotragung und Schadenerledigung beim Bund

1.2.2 Risikokultur

Eine der wichtigsten Voraussetzungen für ein wirksames und vorausschauendes Risikomanagement ist eine gute «Risikokultur»: Alle Mitarbeitenden und jede Führungskraft pflegen einen bewussten Umgang mit Risiken und eine positive Fehlerkultur.

- ***Umgang mit Fehlern**:* Eine positive Fehlerkultur erlaubt die offene Diskussion über Mängel und fördert die Aufdeckung von Risiken innerhalb von Prozessen und Systemen. Lösungen zur Reduktion dieser Risiken können erarbeitet werden. Eine offene Kommunikation über Fehler erlaubt es zudem, aus den Fehlern anderer zu lernen.

- ***Offener Informationsaustausch und Lernkultur**:* Eine offene Kommunikation, unter Berücksichtigung der Sicherheitsvorschriften klassifizierter Informationen (vgl. Ziffer 1.4), und die Bereitschaft, von anderen zu lernen, fördern ein besseres und tieferes Verständnis der eigenen Aufgaben und Prozesse. Insbesondere die Identifikation und die Bewältigung von Risiken an der Schnittstelle zwischen zwei oder mehreren OE werden so erleichtert. Jeder Bereich profitiert von den Erfahrungen der anderen.

- ***Respekt vor fachlichem Wissen und Können**:* Bei der Risikoanalyse und bei der Erarbeitung von Bewältigungsoptionen wird Wert auf die Meinung der Personen mit grossem Know-how gelegt, auch wenn diese keine Entscheidungsbefugnisse haben. Ihre Stellungnahmen und allenfalls davon abweichende Entscheide der Führung («management overruling») sollen dokumentiert werden.

- ***Informationspflicht**:* Die Pflicht jedes Mitarbeitenden, seine Vorgesetzten über relevante Gefahren in seinem Tätigkeitsbereich zu informieren, führt zu erhöhter Aufmerksamkeit und dazu, dass die Risikoverantwortung wahrgenommen wird.

Neben der Förderung von allgemeinen Arbeitsgrundsätzen, welche die Risikokultur verbessern, ist auch ein regelmässiger Austausch zu Themen des Risikomanagements wichtig. Dieser fördert das Risikobewusstsein und die Sensibilität für das Thema Risikomanagement (vgl. auch Ziff. 5.1).

Selbstverständlich kann der Aufbau bzw. die Verbesserung der Risikokultur nicht von einem Tag auf den anderen erfolgen. Das benötigt seine Zeit, denn Arbeitseinstellungen und Denkmuster können oft nur langsam neu ausgerichtet werden. Die EFV wird diesem Thema im Rahmen der steten Verbesserung des Risikomanagements Bund grosse Aufmerksamkeit schenken und nötigenfalls Massnahmen ergreifen, um weitere Verbesserungen herbeizuführen.

1.3 Geltungsbereich und Risikodefinition

Für den Geltungsbereich und die Risikodefinition wird auf Ziffer 2 der Richtlinien EFV verwiesen.

1.4 Umgang mit als GEHEIM klassifizierten Informationen

Das Risikomanagement befasst sich mit *allen* Aufgabengebieten des Bundes, somit auch mit sehr sensiblen Bereichen wie z.B. der inneren und äusseren Sicherheit. Auch die Risiken aus diesen Bereichen fliessen in die Risikoberichterstattung an den Bundesrat ein. Als GEHEIM klassifizierte Informationen sind in geeigneter Weise im Risikomanagement zu erfassen. Der Schutz von Informationen des Bundes und der Armee im Interesse des Landes und

insbesondere deren Klassifizierung und Bearbeitung ist in der Informationsschutzverordnung[8] geregelt. Zum Thema Klassifizierung von Informationen des Risikomanagements siehe Ziffer 5.3.1 hiernach.

2 Organisation des Risikomanagements Bund

2.1 Aufbau

Das Risikomanagement innerhalb der Bundesverwaltung ist dezentral organisiert. Die Departemente und die BK sind für die Umsetzung in ihrem Bereich verantwortlich. Auf der Stufe Departement / BK und in jeder VE[9] ist je eine Risikomanagement-Funktion vorgesehen, die die verschiedenen Risikomanagement-Tätigkeiten koordiniert und den Risikomanagementprozess steuert. Demgegenüber erfüllt die Koordinationsstelle Risikomanagement in der EFV (Koordinationsstelle EFV) eine departementsübergreifende Funktion. Sie soll sicherstellen, dass das Risikomanagement in der Bundesverwaltung einheitlich umgesetzt wird.

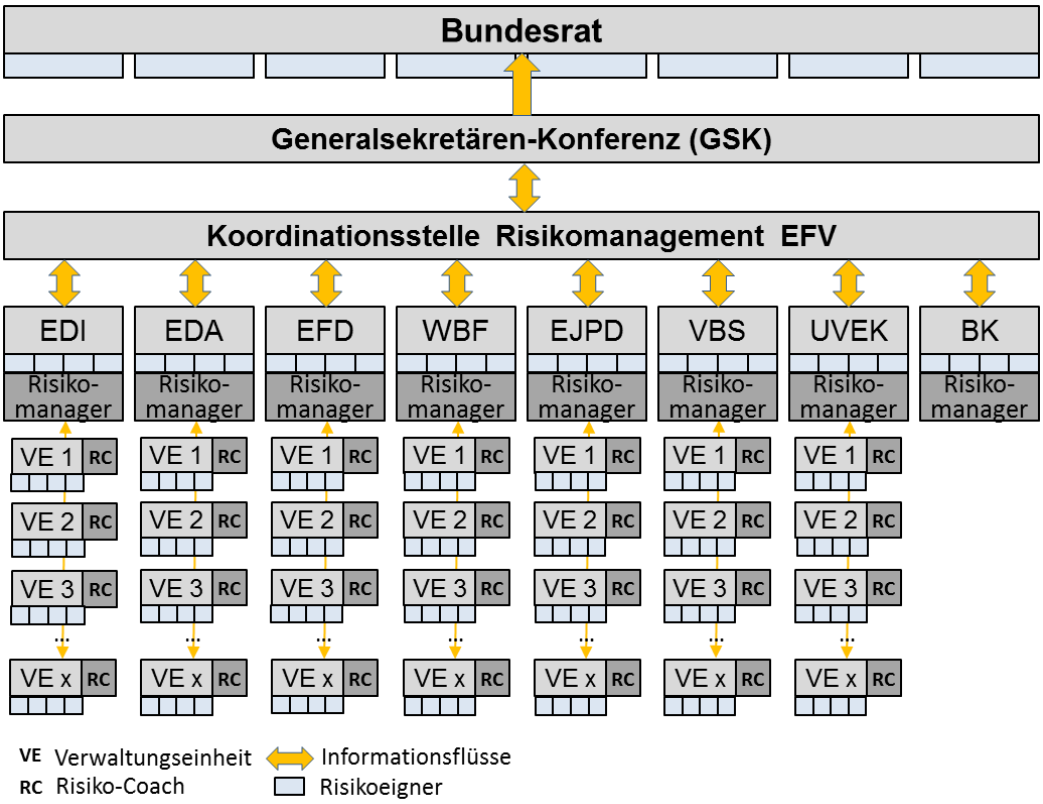


Abbildung 1: Organisation Risikomanagement Bund

2.2 Funktionen und Verantwortlichkeiten

Die Aufgaben und Verantwortlichkeiten der verschiedenen Funktionen im Risikomanagement Bund sind in Ziffer 3 der Richtlinien EFV umschrieben. Die Funktionen beim Bund, für deren

[8] ISchV; SR *510.411*

[9] Das Gleiche gilt für die Generalsekretariate. Die Funktion des Risikocoachs des Generalsekretariats kann (muss aber nicht) in Personalunion vom Risikomanager des Departements ausgeübt werden.

Ausübung eine Personensicherheitsprüfung durchgeführt werden muss (z. B. Risikomanager), sind in Anhang 1 der Verordnung über die Personensicherheitsprüfungen (PSPV; SR *120.4*) aufgeführt.

2.3 Einbettung des Risikomanagements in die Führungsprozesse der Bundesverwaltung

Das Risikomanagement ist ein wichtiges Führungsinstrument des Bundesrates und ein fester Bestandteil der Geschäfts- und Führungsprozesse der Departemente / der BK und der VE und gehört zur sorgfältigen und wirtschaftlichen Aufgabenerfüllung[10]. Mit dieser bundesrätlichen Verpflichtung der Führungskräfte soll sichergestellt werden, dass das Risikomanagement in der Bundesverwaltung auf allen Stufen umgesetzt wird und dass dessen Resultate zur Zielerreichung des Bundes beitragen. Ein integriertes Risikomanagement verbindet und koordiniert diesen Top-down-Ansatz mit dem Bottom-up-Ansatz, der darin besteht, dass Risikoanalyse und Risikobewältigung dezentral auf der Stufe der einzelnen OE erfolgen. Ein integriertes Risikomanagement wird so zu einem effektiven Instrument zur Führung der Bundesverwaltung.

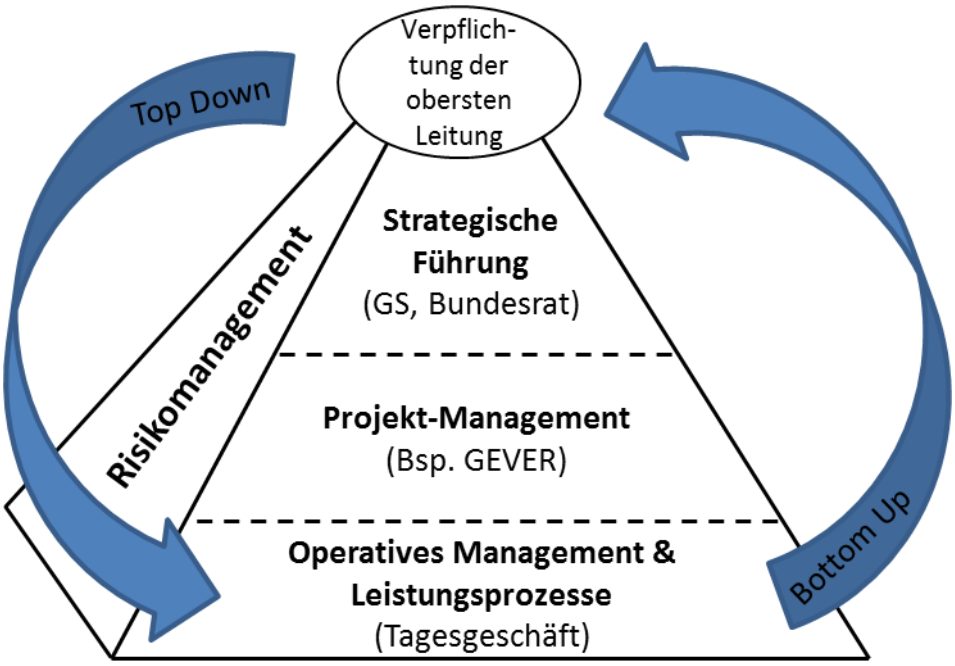


Abbildung 2: Integriertes Risikomanagement

2.3.1 Strategie- und Planungsprozesse

Mit der Legislaturplanung und den jährlich festgelegten Zielen des Bundesrates soll der Bund rechtzeitig auf Veränderungen des Umfeldes reagieren. Der Perspektivstab unterstützt den Bundesrat dabei mit regelmässigen Umfeld- und Lageanalysen (vgl. Ziff. 6.4). Diese erläutern die wichtigsten künftigen Herausforderungen für die Bundespolitik. Es ist wichtig, dass zwischen dem Perspektivstab und dem Risikomanagement Bund ein Informationsaustausch stattfindet, damit die sich am Horizont abzeichnenden Gefahren und Bedrohungen möglichst frühzeitig als mögliche Risiken erfasst und bewirtschaftet werden können. Auch auf den Stufen Departement / BK und VE soll der Strategieprozess mit dem Risikomanagement vernetzt

[10] Ziff. 4 Abs. 1 der Weisungen

werden.
Die Finanzplanung und der Voranschlag (Budget) sind ebenfalls wesentliche Steuerungselemente in der Bundesverwaltung.

2.3.2 Weitere Prozesse

Weiter existieren auf unterschiedlichen Stufen, zum Teil nur in einzelnen OE, diverse Prozesse, wie das IKS, das Qualitätsmanagement, das Umweltmanagement, das Arbeitssicherheitsmanagement und das IT-Sicherheitsmanagement. Synergien zwischen diesen Prozessen und dem Risikomanagement müssen gefunden und genutzt und die Prozesse müssen vernetzt werden. In allen Fällen ist der Informationsaustausch sicherzustellen.

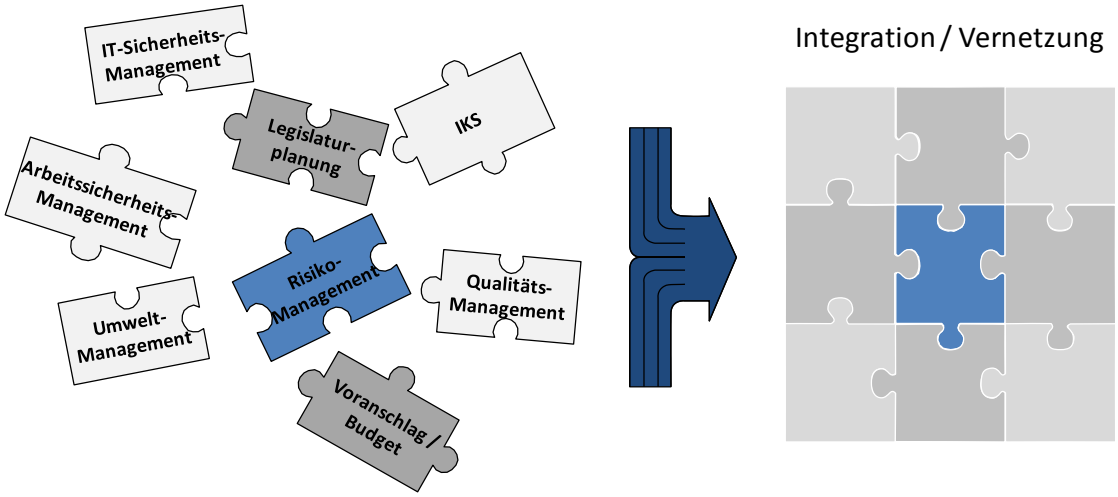


Abbildung 3: Vernetzung von Führungsprozessen in der Bundesverwaltung

Definition der Rahmenbedingungen:
Empfehlung EFV:

- Die EFV empfiehlt den Risikomanager und Risikocoaches, den Strategie- und den Controlling-Prozess (Finanzplanung und Voranschlag) mit dem Risikomanagementprozess in ihrer OE zu vernetzen und abzuklären, welche Schnittstellen und weitere Prozesse (IKS, Qualitätsmanagement, IT-Sicherheitsmanagement usw.) berücksichtigt und in die Planung mit einbezogen werden müssen.

3 Risikomanagementprozess

Die Konsolidierung der Risiken auf Stufe Departement / BK und Bundesrat setzt voraus, dass die Bewertungen der einzelnen Risiken untereinander vergleichbar sind. Die Identifikation, Analyse und Bewertung, Beurteilung, Bewältigung und Überwachung der Risiken muss deshalb nach einheitlichen Regeln erfolgen. Diese werden mit den Richtlinien EFV verbindlich vorgegeben. Zur Unterstützung einer einheitlichen Umsetzung des Risikomanagementprozesses in der Bundesverwaltung und zur Ermöglichung eines Reportings auf Stufe Bundesrat und Departement / BK wird für die Bewirtschaftung der Risiken und die Risikoberichterstattung eine gemeinsame Informatikanwendung (R2C) verwendet[11]. Diese wird von der EFV zur Verfügung gestellt und betreut.

[11] Ziff. 3 Abs. 1 der Weisungen

In dieser und den nachfolgenden Ziffern wird die Umsetzung der Aufgaben innerhalb des Risikomanagementprozesses (vgl. Abbildung 4) in der Bundesverwaltung erläutert.

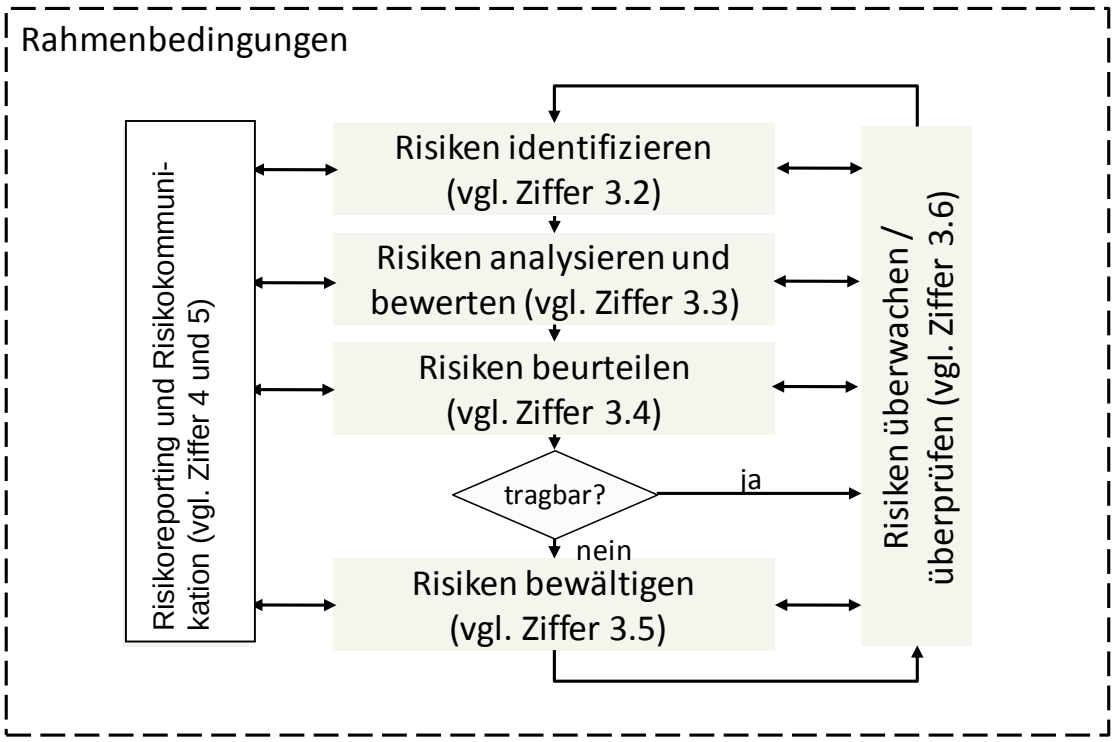

Rahmenbedingungen
Risikoreporting und Risikokommuni-kation (vgl. Ziffer 4 und 5)
Risiken identifizieren (vgl. Ziffer 3.2)
Risiken analysieren und bewerten (vgl. Ziffer 3.3)
Risiken beurteilen (vgl. Ziffer 3.4)
tragbar?
ja
nein
Risiken bewältigen (vgl. Ziffer 3.5)
Risiken überwachen / überprüfen (vgl. Ziffer 3.6)

Abbildung 4: Risikomanagementprozess nach gängigen Normen

3.1 Prozessabläufe und Informationsflüsse in der Bundesverwaltung

Die Prozessabläufe können schematisch wie folgt dargestellt werden:

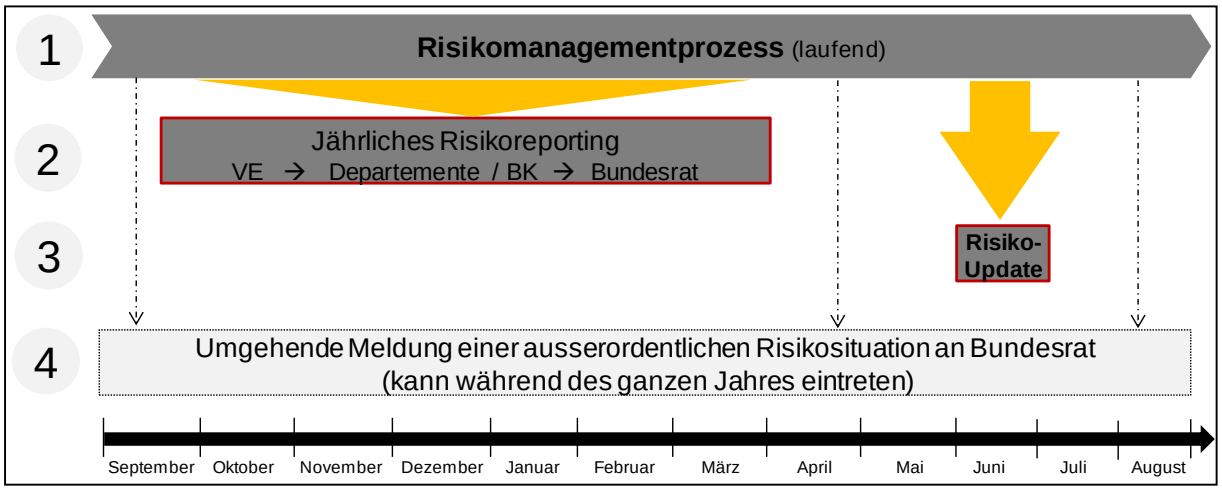


Abbildung 5: Prozessabläufe im Risikomanagement Bund

Die Überwachung der Risikosituation des Bundes durch die Mitarbeitenden und Führungs-

kräfte erfolgt laufend (1). Zusätzlich zum jährlichen bundesweiten Risikoreporting (2) wird betreffend die grössten Risiken des Bundes ein Risiko-Update durchgeführt (3). Bei ausserordentlichen Risikosituationen wird der Bundesrat umgehend informiert (4).[12]

3.1.1 Jährliches Risikoreporting

In der Bundesverwaltung wird einmal jährlich ein *umfassendes* Risikoreporting durchgeführt (vgl. Abbildung 5). Es ist Sache der Risikocoaches und der Risikomanager, für ihre OE die internen Abläufe und Termine im Detail festzulegen. Die Koordinationsstelle EFV gibt nur das Datum für die Abgabe der Departementsreportings verbindlich vor.

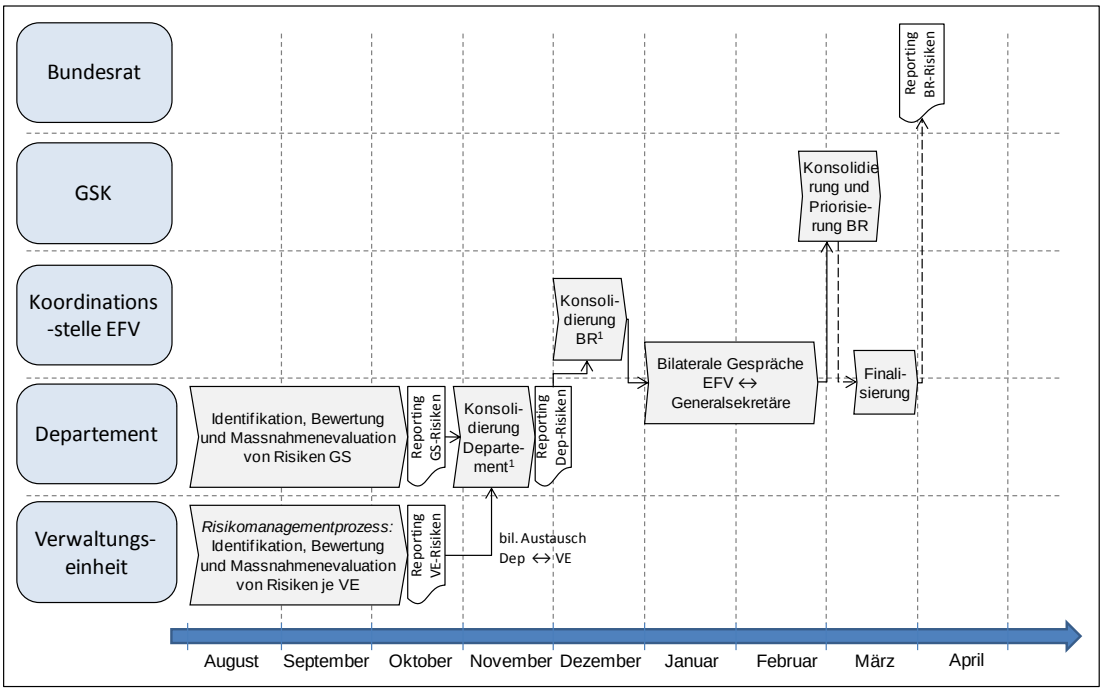


Abbildung 6: Prozessablauf des jährlichen Risikoreportings in der Bundesverwaltung

Die Risikoberichterstattung an den Bundesrat wird von einer Arbeitsgruppe der Geschäftsprüfungskommissionen (GPK) im Rahmen einer Sitzung im April behandelt.

3.1.2 Risiko-Update

Zwecks Dynamisierung und Stärkung des Risikomanagements im Bund wird zusätzlich im Juni ein Risiko-Update durchgeführt. Es handelt sich um einen Top-down-Prozess, der auf die grössten Risiken des Bundes fokussiert. Geprüft wird, ob sich die Kernrisiken der Departemente und der BK verschärft haben und ob zusätzliche Massnahmen eingeleitet werden müssen. Zudem sind Risiken zu melden, die seit dem letzten Risikoreporting neu aufgetaucht und als Kernrisiko des Bundes zu klassifizieren sind oder die Krisenpotenzial aufweisen. Der Bundesrat wird über die Ergebnisse des Risiko-Updates mittels Informationsnotiz orientiert.

[12] vgl. Ziff. 5 Abs. 4 der Weisungen; flankierend wird die Koordinationsstelle EFV informiert.

3.1.3 Informationsflüsse im Risikomanagement Bund

Die nachfolgende Abbildung verdeutlicht schematisch die wichtigsten Informationsflüsse innerhalb des Risikomanagements bis auf Stufe VE.

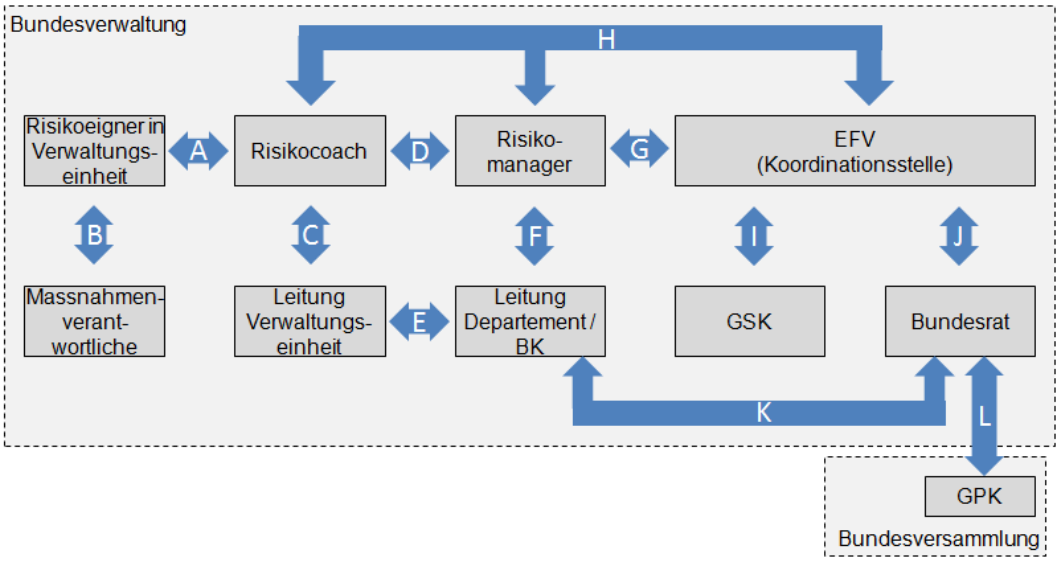


Abbildung 7: Informationsflüsse

Die einzelnen Informationsbeziehungen können wie folgt beschrieben werden:

A Im jährlichen Risikomanagementprozess arbeitet der Risikocoach mit den unterschiedlichen Risikoeignern der VE zusammen, um neue Risiken zu identifizieren, zu analysieren und zu bewerten, zu bewältigen sowie um bereits identifizierte Risiken zu aktualisieren.

B Der Risikoeigner[13] erteilt dem Massnahmenverantwortlichen den Auftrag zur Umsetzung einer Massnahme und überwacht die Umsetzung. Der Massnahmenverantwortliche berichtet dem Risikoeigner periodisch über den Stand der Umsetzung und allfällige Probleme und Verzögerungen.

C Der Risikocoach erstellt zuhanden der Leitung der VE einen Entwurf des Risikoreportings. Diese analysiert und ergänzt die Risiken. Weiter beschliesst sie über die Umsetzung von Massnahmen in ihrem Zuständigkeitsbereich.

D Regelmässiger fachlicher Austausch. Der Risikomanager erlässt terminliche und methodische Vorgaben. Die Risikocoaches liefern dem entsprechenden Risikomanager die Departementsrisiken ihrer VE.

E Information/Diskussion über die Toprisiken der VE, die an das Departement gemeldet werden. Besprechung/Beschlussfassung über Risiko-Massnahmen auf Stufe Departement.

F Der Risikomanager konsolidiert die Risiken aller VE und erstellt zuhanden der Leitung des Departement / der BK einen Entwurf des Risikoreportings. Diese analysiert und ergänzt die Risiken. Weiter verabschiedet sie das Departementsreporting zuhanden des Bundesrats via Koordinationsstelle EFV.

G Regelmässiger fachlicher Erfahrungsaustausch. Die Koordinationsstelle EFV erlässt

[13] Der Risikoeigner kann auch die Leitung der VE oder des Departements / der BK sein.

terminliche und methodische Vorgaben. Die Risikomanager liefern der Koordinationsstelle EFV die Kernrisiken ihres Departements / der BK.

H Fachliche Schulung der Risikomanager und Risikocoaches (Kurs «Risiken verstehen und bewältigen») sowie Schulung und Unterstützung zur Benützung der gemeinsamen Risiko-Informatikanwendung R2C (Risk-to-Chance).

I Die Koordinationsstelle EFV erstellt zuhanden der GSK einen Entwurf des Risikoreportings an den Bundesrat. Die GSK konsolidiert und priorisiert die Risiken aus den Departementen und der BK, analysiert Wechselwirkungen und verabschiedet die Risikoberichterstattung zuhanden des Bundesrats.

J Die Koordinationsstelle EFV finalisiert die Risikoberichterstattung und bringt sie via EFD dem Bundesrat zur Kenntnis.

K Informationsrückfluss aus der Bundesratssitzung an die Leitung des Departments / der BK; allenfalls Auftrag zur Umsetzung von Risiko-Massnahmen auf Stufe Bundesrat.

L Jährliche Besprechung des Bundesrat-Risikoreportings mit einem Ausschuss der GPK.

Definition der Rahmenbedingungen:
Vorgaben EFV:
- Innerhalb des Risikomanagementprozesses müssen die Prozesse und Termine der VE mit dem übergeordneten Departements- und dem bundesweiten Prozess abgestimmt werden.
- In der Bundesverwaltung wird einmal jährlich auf Stufe Bundesrat, Departement / BK und VE ein Risikoreporting erstellt.
- Ein zusätzliches Risiko-Update beschränkt sich auf Bundesratsrisiken und Risiken mit Krisenpotenzial.
- Bei einer ausserordentlichen Risikosituation wird der Bundesrat umgehend informiert.

3.2 Identifikation

3.2.1 Ausgangspunkte und Abgrenzung

Die Risikoidentifikation besteht darin, frühzeitig mögliche Ereignisse und Entwicklungen zu erkennen, welche die Erfüllung der Aufgaben und die Erreichung der Ziele des Bundes beeinträchtigen können. Neben Ereignissen, die sich kurzfristig realisieren können, sind auch langfristige Entwicklungen zu beachten. Um eine verlässliche, nicht dem Zufall überlassene Risikoidentifikation sicherzustellen, braucht es einen *systematischen*, periodisch durchgeführten Prozess. Dieser ergänzt die stete Aufmerksamkeit der Mitarbeiterinnen und Mitarbeiter des Bundes gegenüber neuen Entwicklungen, die negative Auswirkungen auf die Bundesverwaltung haben können.

Als Ausgangspunkte für die systematische Risikoidentifikation dienen:
- die sich aus der Bundesverfassung und den Gesetzen ergebenden Ziele und Aufgaben;
- die in den Organisationsverordnungen der Departemente und der BK aufgelisteten Ziele und Funktionen; und

- die Jahresziele des Bundesrates, der Departemente / der BK und der VE.

Nebst den Aufgaben und Zielen des Bundes können ergänzend auch *Prozessdiagramme* herangezogen werden, falls eine VE zwecks Eruierung von Schwachstellen und Einwirkungsorten von Risiken innerhalb eines spezifischen Prozesses solche verwendet. Laufende Projekte sind auch Gegenstand des Risikomanagementprozesses.

Bei der Suche und Identifikation von Risiken, welche die Aufgabenerfüllung oder die Zielerreichung des Bundes gefährden oder negativ beeinflussen können, muss jeweils im Detail analysiert werden, ob und inwiefern *für den Bund* ein Risiko vorliegt. Nachfolgend zwei Beispiele, die die Problematik der Abgrenzung eines Bundesrisikos veranschaulichen sollen.

Pandemie:

- Für die volkswirtschaftlichen Schäden, die sich bei einer Pandemie ergeben (Produktivitätsverluste, zusätzliche Gesundheitskosten), ist der Bund grundsätzlich nicht verantwortlich.
- Dem Bundesamt für Gesundheit (BAG) obliegen im Zusammenhang mit der Früherkennung von neuen Bedrohungen für die Gesundheit eine ganze Reihe von Aufgaben[14]. Ein Risiko für das BAG (und somit für den Bund) kann demzufolge darin liegen, dass es dem BAG beispielsweise nicht gelingt, eine Pandemie frühzeitig zu erkennen und die Bevölkerung mit den notwendigen Informationen zu versorgen.
- Von einer Pandemie können Mitarbeiter der gesamten Bundesverwaltung betroffen sein. Fallen diese krankheitshalber in grösserer Zahl aus, ist die Aufgabenerfüllung in mehreren VE möglicherweise in Frage gestellt, was für den Bund ein weiteres Risiko darstellt.

Konkurs einer Grossbank:

- Der Konkurs einer Grossbank in der Schweiz und dessen direkte Auswirkungen (z. B. Verluste für Gläubiger und Investoren) sind grundsätzlich kein Risiko des Bundes.
- Die Förderung der Stabilität des schweizerischen Finanzsektors ist eine der Aufgaben des Staatssekretariats für internationale Finanzfragen[15]. Ist ein Institut «systemrelevant» (too big to fail), sodass dessen Ausfall das schweizerische Finanzsystem gefährden oder lahmlegen könnte, so betrifft das Risiko auch den Bund; er müsste gegebenenfalls Rettungsmassnahmen in die Wege leiten.

3.2.2 Vorgehen

Die Risiken in der Bundesverwaltung sind sehr vielfältig. Um eine Unterteilung der Risiken zu ermöglichen und die Identifikation systematisch durchzuführen werden in der Bundesverwaltung die die Risiken *aufgrund ihrer Ursache* in folgende sechs Kategorien unterteilt[16]:

- ***finanzielle und wirtschaftliche Risiken****:* Risiken im Zusammenhang mit dem Finanzmanagement, mit (wirtschaftlichen) Abhängigkeiten des Bundes von Dritten, mit subsidiären Leistungen des Bundes (Darlehen, Bürgschaften, Garantien usw.);
- ***rechtliche Risiken / Compliance****:* Risiken im Zusammenhang mit Schäden anlässlich des Vollzugs von Bundesaufgaben, mit der Einhaltung von rechtlichen Bestimmungen oder Verträgen, mit Aufsichtspflichtverletzungen, mit der Ausfallhaftung nach Art. 19 VG[17] usw.;

[14] Art. 9 Organisationsverordnung für das EDI (SR *172.212.1*)
[15] Art. 7 Abs. 1 Bst. b Organisationsverordnung für das EFD (SR *172.215.1*)
[16] Weitere Möglichkeiten, mehrere Risiken zu strukturieren oder zu gruppieren, werden im Anhang 3 erläutert.
[17] In Anhang 7 werden einige Risiken des Bundes im Zusammenhang mit Organisationen ausserhalb der Bundesverwaltung aus rechtlicher Perspektive genauer erläutert.

- ***Sach-, technische und Elementarrisiken**:* Risiko der Zerstörung oder Beschädigung (inklusive Betriebsunterbruch) von bundeseigenen Gebäuden, Einrichtungen, technischen Anlagen, Daten, Kulturgütern;
- ***personenbezogene und organisatorische Risiken**:* Risiken aus den Bereichen Organisation, Führung, Mitarbeiter, Personenschutz, Rekrutierung von Fachkräften, Ausfall von Schlüsselpersonen, Veruntreuung;
- ***technologische und naturwissenschaftliche Risiken**:* Risiken, die sich aus der Entwicklung und Forschung von technologischen/naturwissenschaftlichen Neuanwendungen (inklusive Spätfolgen) ergeben, wie beispielsweise Nano- oder Gentechnologie;
- ***gesellschaftliche und politische Risiken**:* gesellschaftliche Veränderungen (z. B. Demografie), Interessenkonflikte mit dem Ausland usw. In dieser Kategorie finden sich komplexe Risiken, wie z. B.: Ausstieg Atomenergie, Nanotechnologie, Bilaterale Verträge mit der EU.

Für die Identifikation von Risiken hat sich in der Praxis ein strukturiertes Brainstorming gut bewährt, bei dem anlehnend an die Ziele, Aufgaben und Prozesse[18] nach konkreten Risiken in der untersuchten OE gesucht wird. Dabei kann das Brainstorming sowohl mit Einzel- als auch mit Gruppeninterviews durchgeführt werden.

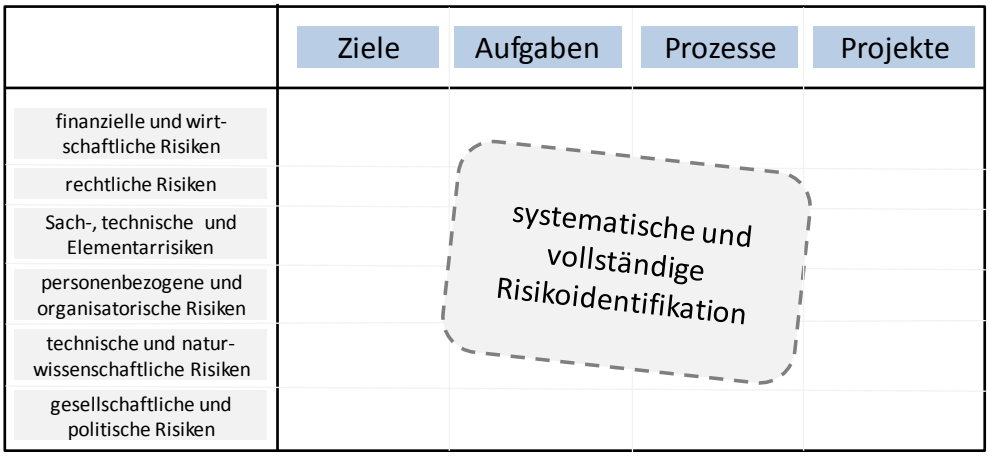


Abbildung 8: Risikoidentifikation

Trotz einer seriösen Risikoidentifikation werden immer sogenannte *Restrisiken* verbleiben, die nicht erkannt und somit nicht bewirtschaftet werden können.[19]

Output Identifikation: Eine möglichst umfassende Liste von Risiken, welche die Erfüllung der Aufgaben und die Erreichung der Ziele des Bundes negativ beeinflussen können.

Hilfsmittel: Risikoerfassungsbogen (vgl. Anhang 2), Prozessbeschriebe.

Prozessschritt Risikoidentifikation:
Vorgaben EFV:
- Die Identifikation der Risiken ist *ausgehend von den Zielen und Aufgaben der Organisationseinheit* durchzuführen (vgl. Bundesverfassung, Gesetze, Verordnungen,

[18] Gefahrenlisten aus dem Qualitätsmanagementsystem, der Arbeitssicherheit, IT-Sicherheitsmanagement usw. sollen – sofern vorhanden – beigezogen werden.
[19] Das Nichterkennen von Risiken kann u. a. aufgrund von Betriebsblindheit passieren, oder dadurch, dass ganz neue und für die Menschen unerwartete Phänomene auftauchen (sogenannte schwarze Schwäne).

Organisationsverordnung des Departements / der BK, Jahresziele, Geschäftsordnung der VE).
- Die Risiken werden in die sechs (vorgenannten) thematischen Risikokategorien unterteilt. Die Zuordnung zu den Kategorien erfolgt aufgrund der Ursache des Risikos.

Empfehlung EFV:
- Durchführung von Workshops oder Interviews mit Mitgliedern der Leitung sowie Mitarbeitenden, welche für spezielle Bereiche zuständig sind (Wissensträger).

3.3 Analyse und Bewertung

3.3.1 Allgemeines zum Erfassen von Risiken

Die Risiken des Bundes werden mit Hilfe der Informatikanwendung Risk-to-Chance (R2C) elektronisch erfasst und dokumentiert. Die periodischen Aktualisierungen der Einzelrisiken werden historisiert.

Prozessschritt Risikoanalyse und -bewertung:
Vorgabe EFV: Jedes Risiko wird mindestens mit folgenden Angaben erfasst:
- prägnanter Risikotitel: kurz, aber auch für Dritte verständlich (vgl. Ziff. 3.2)
- Risikokategorie (vgl. Ziff. 3.2)
- detaillierte Beschreibung des Risikos (Szenario)
- Risikoeigner
- betroffene Organisationseinheit
- Risikoursachen
- Bewertung des Risikos (Auswirkungen und Eintrittswahrscheinlichkeit)
- Erläuterungen und Begründung zur Bewertung des Risikos
- bereits umgesetzte Massnahmen zur Risikominimierung
- zu ergreifende Massnahmen zur Risikominimierung (insbesondere Stand der Umsetzung, Massnahmenverantwortlicher, Kosten/Nutzen)
- allfällige Wechselwirkungen mit anderen Risiken.

3.3.2 Methoden zur Analyse und Bewertung von Risiken

Bei der Risikoanalyse geht es vorab darum, das identifizierte Risiko (auch für Aussenstehende) verständlich zu beschreiben, Ursachen und Auswirkungen zu ermitteln und Zusammenhänge zu verstehen (inkl. Wechselwirkungen mit anderen Risiken, vgl. Ziff. 3.3.7 und 4.5). Schliesslich werden die Eintrittswahrscheinlichkeit und die Auswirkungen des Risikos qualitativ oder quantitativ bewertet. Für die Analyse der Risiken soll das beste verfügbare Know-how verwendet werden, bei Bedarf und verhältnismässigem Aufwand soll auch bundesverwaltungsexternes Know-how mit einbezogen werden.

Da Risiken sehr unterschiedlich sein können, hat die Praxis für ihre Analyse und Bewertung mehrere Methoden entwickelt. Einige sollen hier kurz erläutert werden.[20]

- **Szenarioanalysen**: Bei den Szenarioanalysen werden Ursachen von identifizierten Risiken ermittelt und die Auswirkungen von einzelnen Szenarien eingeschätzt und dargestellt. Ziel ist es, die Ursache-Wirkungsketten vor und nach dem Eintritt eines Risikos zu verstehen. In den meisten Fällen wird dabei ein sog. «credible worst

[20] Vgl. dazu z. B. ONR 49002-2

case»-Szenario zur Darstellung des Risikos verwendet (vgl. Ziff. 3.3.3). Spezifische Formen der Szenarioanalysen sind das «Ursache-Wirkungsdiagramm» (verwendet zur Analyse von eingetretenen Schadenereignissen), und die «Fehlerbaum- und Ablaufanalyse» (verwendet bei komplexen technischen Systemen).

- **Indikatorenanalysen**: Bei der Indikatorenanalyse wird versucht, Indikatoren bzw. Vorkommnisse, die beinahe zu einem Schaden geführt hätten, zu erkennen. Sie können auf das mögliche Eintreten eines worst-case-Risikoszenarios hinweisen. Durch die Analyse dieser Vorkommnisse bzw. Indikatoren können Massnahmen zur Risikominimierung gefunden und umgesetzt werden. Eine spezifische Form einer Indikatorenanalyse ist das «Change Based Risk Management», bei dem *Veränderungen* identifiziert, systematisch bewertet und deren Einfluss auf die Organisation analysiert werden.

- **Funktionsanalysen**: Bei einer Funktionsanalyse wird das untersuchte Objekt (meist ein technisches System oder ein Prozess) in Teilsysteme/-prozesse zerlegt und deren Funktionen/Aufgaben ermittelt. Danach wird nach möglichen Fehlfunktionen (und deren Ursachen) gesucht, die die Funktionsfähigkeit der Teilsysteme und des Gesamtsystems beeinträchtigen können. Eine häufig verwendete Funktionsanalyse ist die «Failure Mode and Effects Analysis» (FMEA).

- **Statistische Analysen**: Bei den statistischen Analysen wird das Risiko als statistisches Mass der Unsicherheit betrachtet. Diese Analysen bedingen eine gute und genügend grosse Datengrundlage. Gebräuchliche Risikokennzahlen sind die Standardabweichung und der Value-at-Risk. Mit einer Monte Carlo-Simulation lassen sich Risiken in einem wiederholten Zufallsprozess simulieren und eine Schadensverteilung eines Risikos oder einer aggregierten Gruppe von Risiken ermitteln.

Während die Szenarioanalyse eine allgemein anwendbare Methode ist, die sich zudem gut für eine Top-down-Analyse eignet, sind einige der anderen hiervor erwähnten Methoden nur sehr spezifisch anwendbar.

Prozessschritt Risikoanalyse und -bewertung:
Vorgabe EFV:
- In der Bundesverwaltung werden die Risiken mit Hilfe der Szenarioanalyse dargestellt. Andere Analysemethoden sind fakultativ.

Empfehlung EFV:
- Für die Analyse der Risiken soll das beste verfügbare Know-how verwendet werden, bei Bedarf und verhältnismässigem Aufwand soll auch bundesverwaltungsexternes Know-how mit einbezogen werden.

3.3.3 Schadensverteilung eines Risikos

Die meisten Risiken können sich in unterschiedlichem Ausmass realisieren: Ein Hochwasser kann sich als lokales Ereignis mit moderatem Sachschaden manifestieren, das häufig vorkommen kann, oder als sehr seltenes «Jahrhunderthochwasser» mit gravierenden Auswirkungen. Es gibt generell drei Möglichkeiten den unterschiedlichen Ausprägungen eines Risikos Rechnung zu tragen:

- ***Schadensverteilung**:* Bei Vorliegen statistischer Daten oder bei einem genügenden Verständnis des Risikos kann dieses mit einer genauen Schadensverteilung beschrieben werden.
- ***Szenarien**:* Szenarien sind eine gute Annäherung. Häufig werden drei Szenarien dargestellt, die zusammen die ganze Bandbreite des Risikos abbilden.

- ***«Credible worst case»**:* Das Risiko wird in der schlimmst möglichen aber noch realistischen Ausprägung dargestellt. Es wird derjenige Fall abgebildet, welcher der Organisation die grössten Schwierigkeiten bereiten kann.

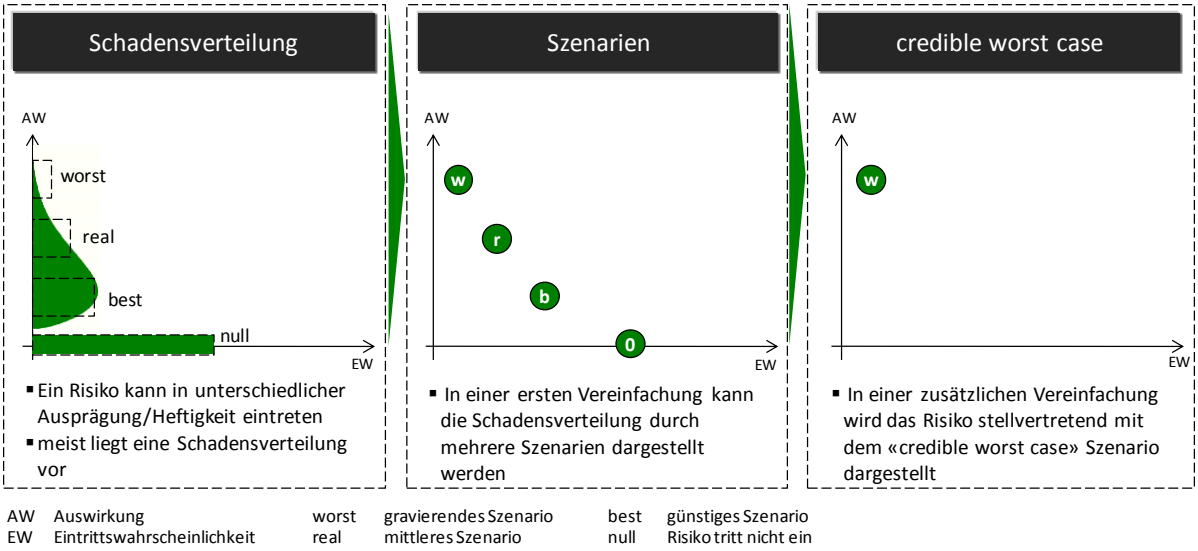


Abbildung 9: Schadensverteilung eines Risikos

Prozessschritt Risikoanalyse und -bewertung:
Vorgabe EFV:
- In der Bundesverwaltung wird das Risiko als «credible worst case» dargestellt. Bei Bedarf und für ein besseres Verständnis des Risikos können zusätzlich auch mehrere Szenarien oder eine Schadensverteilung dargestellt werden.

3.3.4 Bewertung der Auswirkungen

Die Auswirkungen eines Risikos können vielfältig und verschiedenartig sein. Aus Sicht Risikomanagement Bund sind oft gleichzeitig verschiedene Auswirkungsdimensionen von Bedeutung. Im Einvernehmen mit den Risikomanager der Departemente und der BK wurde festgelegt, dass die Auswirkungen der Risiken mit den folgenden fünf Dimensionen beschrieben werden sollen:

- finanzielle Auswirkungen
- Personenschäden
- Beeinträchtigung der Reputation
- Beeinträchtigung der Geschäftsprozesse
- Auswirkungen auf die Umwelt

In allen fünf Dimensionen muss das Risiko bezüglich der Höhe der Auswirkungen auf einer sechsstufigen Skala von «sehr gering» bis «sehr hoch» bewertet werden (vgl. Bewertungsmatrix Risikomanagement Bund), wenn die Auswirkungsdimension für das Risiko relevant ist. Jede Dimension hat verglichen mit den anderen das gleiche Gewicht, die gleiche Bedeutung. Das Risiko ist unter Berücksichtigung aller relevanten Auswirkungsdimensionen einzustufen. Wenn mehrere Dimensionen von Bedeutung sind, wird das Risiko in einer ***Gesamtbewertung*** entsprechend der höchsten Auswirkung eingestuft. Im folgenden Beispiel (Gesamteinstufung hoch) wird das Prinzip der Gesamtbewertung verdeutlicht.

Auswirkungen	sehr gering	gering	moderat	wesentlich	hoch	sehr hoch
Finanzielle Auswirkungen				X		
Personenschäden					X	
Beeinträchtigung Reputation				X		
Beeinträchtigung Geschäftsprozesse			X			
Auswirkungen auf Umwelt						

Abbildung 10: Gesamtbewertung der Auswirkung

Bereits umgesetzte Massnahmen zur Verminderung eines Risikos werden bei der Bewertung der Auswirkungen berücksichtigt (Grundsatz der ***Nettobewertung***).

In der Bewertungsmatrix wird nur die Bewertungsskala auf Stufe Bund und Departement / BK festgelegt. In den VE können den konkreten Bedürfnissen (Grösse des Budgets, spezielle Charakteristiken der Risiken, usw.) besser angepasste Skalen verwendet werden.[21] Die EFV befürwortet solche Individualisierungen der Bewertungsskala, da auf diese Weise in den VE das Risikomanagement als Führungs- und Arbeitsinstrument gestärkt wird.

Prozessschritt Risikoanalyse und -bewertung:
Vorgaben EFV:
- Jedes Risiko ist bezüglich den fünf Auswirkungsdimensionen zu bewerten. Das Risiko wird gesamthaft entsprechend der höchsten Auswirkung eingestuft.
- Bereits wirksame Risikominimierungsmassnahmen sind bei der Bewertung zu berücksichtigen.

Empfehlung EFV:
- Die EFV empfiehlt die Einführung von bedürfnisgerecht angepassten Bewertungsskalen der Auswirkungen pro VE.

3.3.5 Qualitative oder quantitative Bewertung

Ein Risiko kann grundsätzlich anhand von vordefinierten Abstufungen grob (qualitativ) zugeordnet oder quantitativ bewertet werden. Eine quantitative Bewertung ist in der Regel nur dann zweckmässig, wenn die Datenlage sehr gut ist (z. B. vorhandene statistische Angaben über Schadenfälle) und ausschliesslich mit finanziellen Auswirkungen gerechnet werden muss.

Prozessschritt Risikoanalyse und -bewertung:
Empfehlung EFV:
- Die EFV empfiehlt, die Risiken *qualitativ* zu bewerten, unter Berücksichtigung der fünf Auswirkungsdimensionen.

[21] Die technische Umsetzung in R2C erfolgt durch die EFV.

3.3.6 Bewertung der Eintrittswahrscheinlichkeit

Ein Risiko ist per Definition ein unsicheres Ereignis. Dessen Eintrittswahrscheinlichkeit liegt zwischen 0 und 100 Prozent. Dieser Prozentwert kann auf zwei verschiedene Arten interpretiert werden:

a. Eine Eintrittswahrscheinlichkeit von 10 % kann zum Beispiel bedeuten, dass in einem Jahr das Risiko mit 10 %-iger Eintrittswahrscheinlichkeit eintritt bzw. dass sich im Durchschnitt in 10 Jahren das Risiko einmal realisiert. Wir sprechen von einer Periodenwahrscheinlichkeit bzw. einer *Jahreswahrscheinlichkeit*. In dieser Interpretation kann das Risiko über einen längeren Zeithorizont mehr als einmal auftreten. Beispiele sind die meisten operativen Risiken, die häufig durch Ereignisse ausgelöst werden.
b. Eine Eintrittswahrscheinlichkeit von 10 % kann auch als *Fallwahrscheinlichkeit* interpretiert werden. Ein Beispiel einer Fallwahrscheinlichkeit ist ein Risiko, das entweder eintreten kann oder ausbleibt, aber nicht mehrmals auftreten kann. Dies können zum Beispiel strategisch-politische Risiken sein, die durch eine negative Entwicklung ausgelöst werden. Aufgrund eines dynamischen Umfelds haben solche Risiken häufig einen einmaligen Charakter. Weiter ist auch die Eintrittswahrscheinlichkeit, dass ein spezifisches Projekt scheitert, als Fallwahrscheinlichkeit zu interpretieren.

Diesen unterschiedlichen Interpretationen muss beim Vergleichen von Risiken Rechnung getragen werden, indem beispielsweise in der Beschreibung des Risikos erklärt wird, ob es mehrmals eintreten kann und gegebenenfalls in welchem Zeitraum. Damit die Riskmap bezüglich der Eintrittswahrscheinlichkeit aussagekräftig ist, müsste man streng genommen Risiken mit Periodenwahrscheinlichkeit und solche mit Fallwahrscheinlichkeit trennen. Auf Stufe Bundesrat wird aus Gründen der Praktikabilität auf diese Unterteilung verzichtet. Die Eintrittswahrscheinlichkeit ist als Fallwahrscheinlichkeit *und* als Jahreswahrscheinlichkeit zu verstehen und muss je nach Risiko unterschiedlich interpretiert werden.

Die finanziellen Folgen von bekanntermassen *mehrmals jährlich auftretenden Ereignissen* (sog. Frequenzschäden, z. B. Motorfahrzeugschäden einer Versicherung) sind mit einem Jahresdurchschnittswert zu budgetieren. Das Risiko besteht dann in einer allfälligen Überschreitung des budgetierten Wertes im betreffenden Jahr. Dieses Risiko stellt ein unsicheres Ereignis dar und hat somit eine Eintrittswahrscheinlichkeit kleiner 100 %.

Die in der Bundesverwaltung verwendete Eintrittswahrscheinlichkeitsskala ist in der Bewertungsmatrix Risikomanagement Bund abgebildet. Auf VE-spezifische Eintrittswahrscheinlichkeitsskalen wird aus Gründen der Übersichtlichkeit und Vergleichbarkeit verzichtet.

3.3.7 Wechselwirkungen zwischen Risiken

Jedes Risiko muss daraufhin analysiert werden, ob sich bei dessen Eintritt nebst den primären Folgen weitere Auswirkungen auf andere Risiken entfalten. Der Eintritt eines Risikos kann z. B. dazu führen, dass der Eintritt eines weiteren Risikos wesentlich wahrscheinlicher wird (positive Korrelation). Auch das Gegenteil gibt es: Die Eintrittswahrscheinlichkeit eines anderen Risikos kann den Eintritt eines anderen unwahrscheinlicher machen (negative Korrelation). Generell ist zu prüfen, ob ein Zusammenhang mit anderen identifizierten Risiken, allenfalls Risiken in einer anderen VE oder einem anderen Departement, besteht. Wechselwirkungen zwischen Risiken müssen erkannt, möglichst gut verstanden und in der Risikobeschreibung erläutert werden. Eine erste Prüfung auf Wechselwirkungen wird bei der Analyse des Einzelrisikos durchgeführt. Wegen der auf den Stufen Departement / BK und Bundesrat vorhandenen grösseren Übersicht über alle identifizierten Risiken erfolgt eine weitere umfassende Prüfung der Wechselwirkungen zwischen den grösseren Risiken in der Bundesverwaltung durch die Risikomanager, die Koordinationsstelle EFV und die GSK (vgl. Ziff. 4.5).

Prozessschritt Risikoanalyse und -bewertung:
Vorgabe EFV:

- Bei jedem Risiko ist auf den Stufen VE, Departement / BK und Bundesrat zu prüfen, ob Wechselwirkungen mit anderen Risiken bestehen.

Output Risikoanalyse und -bewertung: eine verständliche Beschreibung jedes Risikos und eine Bewertung der Eintrittswahrscheinlichkeit und der Auswirkungen des Risikos.

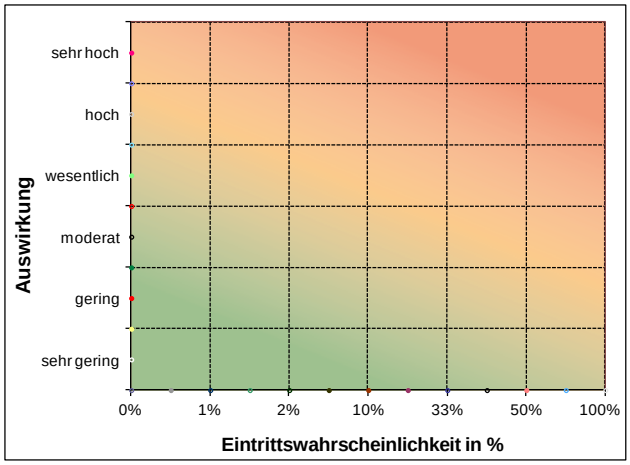
Hilfsmittel: Bewertungsmatrix Risikomanagement Bund.

3.4 Beurteilung

Nachdem die Risiken bewertet worden sind, werden im nächsten Prozessschritt die Bedeutung und die Tragbarkeit der Risiken beurteilt. Einerseits geht es darum herauszufinden, ab welcher Höhe sich das Management mit einem Risiko befassen und Massnahmen ins Auge fassen soll. Andererseits geht es um die Frage, ob die Risiken bei Eintritt mit den eigenen Mitteln getragen werden können.

Risikotoleranz

Mit der Definition der sechs Stufen der Auswirkungen (von «sehr gering» bis «sehr hoch») in der Bewertungsmatrix Bund wird eine grobe Einstufung der Risiken nach ihrer Bedeutung vorgenommen. Die konkrete Bedeutung im Einzelfall hängt u. a. vom Risikokontext und der Grösse der untersuchten Organisationseinheit[22] ab und sollte auf Stufe VE individuell festgelegt werden. Weiter müssen die Leitungen auf den Stufen VE, Departement / BK und Bundesrat definieren, wo ihre Risikotoleranzschwelle liegt.[23] In der nachfolgenden Darstellung wird eine *mögliche* Unterteilung der Risiken in drei Risikotoleranzstufen skizziert.



	Beurteilung
hohes Risiko	Das Risiko stellt eine erhebliche Gefahr dar und muss in der Direktion behandelt werden. Diese setzt sich mit möglichen Massnahmen auseinander und entscheidet bzgl. deren Umsetzung. Das Risiko wird regelmässig verfolgt, solange es sich auf dieser Stufe befindet.
mittleres Risiko	Das Risiko stellt eine ernstzunehmende Gefahr dar. Es muss in der Direktion bekannt sein und von ihr verstanden werden. Die Entwicklung wird verfolgt und wo sinnvoll Massnahmen umgesetzt.
tiefes Risiko	Das Risiko kann akzeptiert werden, es wird innerhalb der Abteilung bewirtschaftet und wo sinnvoll Massnahmen umgesetzt.

Abbildung 11: Beispiel Risikotoleranzstufen

Die Risikotoleranz wird ausserhalb des Risikomanagementprozesses entwickelt. Im Prozess werden lediglich die bewerteten Risiken an diesen Risikotoleranzen gemessen und beurteilt. Selbstverständlich helfen die Toleranzstufen nur, eine *grobe* Idee zu entwickeln, wie mit einem Risiko umgegangen werden soll. Schliesslich muss für jede Bewältigungsmassnahme

[22] Beispielsweise könnten die jährlichen Gesamtausgaben der VE einen groben Indikator zur Beurteilung der *finanziellen* Risikohöhe darstellen.
[23] Die Risikotoleranzschwelle beantwortet die Frage, ab welcher Höhe ein Risiko nicht mehr akzeptiert bzw. getragen werden kann und somit zwingend Risikominimierungsmassnahmen umzusetzen sind.

vor ihrer Umsetzung einzeln beurteilt werden, ob die Kosten der Umsetzung in einem sinnvollen Verhältnis zur Risikoverminderung stehen.

In der Bundesverwaltung wird zur Beurteilung eines Risikos primär die Höhe des Risikos (Auswirkung und Eintrittswahrscheinlichkeit) unter Einbezug der Grösse der VE und deren Aufgaben herangezogen. In Spezialfällen kann das Risiko zusätzlich noch unter Beizug weiterer Dimensionen beurteilt werden:

- Bei Risiken in Finanzmärkten ist eine Rendite-Risiko-Abwägung der Standard, d. h. das getragene Risiko muss in einem sinnvollen Verhältnis zur erwirtschafteten Rendite stehen.
- Im Sicherheitsbereich findet häufig eine Güterabwägung zwischen (Personen-)Risiko und Nutzen statt. Beispielsweise muss bei einem Medikament das Restrisiko (Nebenwirkungen) mit dem Nutzen für die Patienten ins Verhältnis gesetzt werden, um zu einer vernünftigen Beurteilung des Risikos zu gelangen.

Finanzielle Risikotragfähigkeit

Die Bundesverwaltung orientiert sich in ihrer Tätigkeit an ihren Aufgaben und Ziele. Das Gesamtrisiko der Bundesverwaltung ist wesentlich durch die von ihr zu erfüllenden Aufgaben geprägt. Um Risiken zu vermeiden kann demnach nicht auf bestimmte Aufgabenerfüllungen verzichtet werden. Deshalb ist das Gesamtrisiko der Bundesverwaltung hauptsächlich in der Bewirtschaftung der einzelnen Risiken steuerbar. Auf eine Gesamtaggregation aller Risiken in der Bundesverwaltung und der Gegenüberstellung mit dem vorhandenen Kapital wird aus diesem Grund verzichtet.[24]

Die Sicherstellung der Liquidität und Zahlungsfähigkeit der Bundesverwaltung erfolgt durch die Tresorerie in der EFV. Diese kann mit den Tresorerieanlagen monatliche Schwankungen von Einnahmen und Ausgaben von bis zu mehreren Milliarden Franken ausgleichen. Damit kann sie den Eintritt auch von sehr hohen finanziellen Risiken des Risikomanagements (> 1 Mia. CHF) selbst im Fall eines rapiden Geldabflusses decken. Für schweizerische Grossereignisse mit massivem finanziellen Schaden für den Bund (z. B. Kernschmelze in einem AKW, Erdbeben) muss die Liquidität und Aufnahme von Kapital durch den Bund gesondert analysiert werden.

3.5 Bewältigung

3.5.1 Bewältigungsoptionen

Die Risikobewältigung umfasst im Wesentlichen die folgenden unterschiedlichen Handlungsoptionen:

- ***Risiko vermeiden****:* In vielen Fällen kann die Bundesverwaltung ein Risiko nicht komplett vermeiden, denn dies wäre nur durch den Verzicht auf ein Geschäft/Aufgabe möglich, was in den allermeisten Fällen nur über eine entsprechende Gesetzesänderung durchzuführen wäre.

[24] In der Privatwirtschaft orientiert sich die Tragbarkeit von Risiken häufig am vorhandenen (Eigen-) Kapital, d. h. die aggregierten Risiken müssen durch genügend Eigenkapital und liquide Mittel gedeckt und getragen werden können. Ein Gesamtrisiko, das diese Schwelle übersteigt, ist für das Unternehmen existenzgefährdend und somit nicht tragbar. Das Gesamtrisiko kann in diesem Fall gesenkt werden, indem auf bestimmte Tätigkeiten und Geschäfte verzichtet wird oder diese im Umfang wesentlich reduziert werden, oder mittels Aufnahme von zusätzlichem Kapital zur Deckung dieser Risiken.

- ***Risiko vermindern**:* Bei vielen Risiken können mit diversen Massnahmen die Eintrittswahrscheinlichkeit und/oder die möglichen Auswirkungen bei Eintritt des Risikos reduziert werden. Einerseits können Massnahmen präventiv ergriffen werden, andererseits kann die Vorbereitung und der Einsatz eines Krisen- oder eines Kontinuitätsmanagements (vgl. Ziff. 6.2 und 6.3) als Massnahme angesehen werden um ein eingetretenes Risiko möglichst rasch und mit wenig Kosten zu bewältigen.

- ***Risiko überwälzen**:* Einige Risiken können versichert und so auf Dritte übertragen werden. Dies kann unter gewissen Umständen (insbesondere wirtschaftliche Gründe) Sinn machen (vgl. Ziff. 6.6). Derivative Instrumente, Verträge und Garantien bilden weitere Möglichkeiten der Risikoüberwälzung.

In der Bundesverwaltung wird auch nach Umsetzung von Massnahmen häufig ein *Nettorisiko* bleiben, das diese selber trägt. Einerseits kann aus wirtschaftlichen Gründen entschieden werden, das Risiko bewusst selber zu tragen. Andererseits existieren Risiken, die vom Bund getragen werden müssen, weil ein gesetzlicher Auftrag besteht und keine Minimierung des Risikos möglich ist.

3.5.2 Definition, Auswahl und Umsetzung von Massnahmen

Von den Ursachen eines Risikos ausgehend muss der Risikoeigner mit Hilfe des Risikocoaches und von Fachexperten nach möglichen Massnahmen suchen, die das Risiko reduzieren können. Ein genaues Verständnis der Ursachen und der Ursache-Wirkungsketten hilft, geeignete Massnahmen zu finden. Massnahmen müssen klar beschrieben sein, wenn notwendig muss eine Unterteilung in Einzelschritte vorgenommen werden. Zudem muss ein Massnahmenverantwortlicher definiert und ein Endtermin für die Umsetzung festgelegt werden, wenn notwendig mit Zwischenmeilensteinen.

Nach der Identifikation und der Beschreibung von möglichen Massnahmen geht es darum, diese zu beurteilen. Dabei sind die *Kosten* zur Umsetzung der Massnahme mit dem Nutzen, konkret der *Verminderung oder Überwälzung des Risikos*, ins Verhältnis zu setzen. Bei rein finanziellen Auswirkungen kann als grober Ansatz die Reduktion des Risiko-Erwartungswertes[25] mit den Kosten der Massnahme verglichen werden. Bei Risiken mit nicht-finanziellen Auswirkungen erfolgt zwangsläufig eine subjektive Einschätzung des Kosten/Nutzen-Verhältnisses. Diese Einschätzung sollte vom Risikoeigner vorgenommen werden, im Idealfall unterstützt durch Fachpersonen mit dem notwendigen Know-how und unter Berücksichtigung der Risikotoleranz.

Danach werden die als sinnvoll beurteilten Massnahmen priorisiert und über die Umsetzung entschieden. Diese Entscheidung trifft der Risikoeigner bzw., je nach Höhe der Kosten, eine übergeordnete Instanz. Die Umsetzung der Massnahme erfolgt durch den Massnahmenverantwortlichen.

Output Risikobewältigung: Massnahmenliste auf Stufe VE, Departement / BK und Bundesrat.

Prozessschritt Risikobewältigung:
Vorgaben EFV:
- Die Kosten von im Risikomanagement beschlossenen Massnahmen fliessen in das Budget (Voranschlag) des Bundes ein.

[25] Der Erwartungswert eines Risikos ist das Produkt aus finanzieller Auswirkung und Eintrittswahrscheinlichkeit.

- Jede Massnahme muss mit einem Massnahmenverantwortlichen und einem Endtermin versehen sein und eine grobe Kosten/Nutzenanalyse durchgeführt werden.

3.6 Überwachung

Die Überwachung der Risiken und der eingeleiteten Massnahmen ist ein wichtiger Prozessschritt im Risikomanagement, der die Effektivität des Risikomanagements sicherstellt.

3.6.1 Risiko-Überwachung

Mit einer regelmässigen Überwachung der Risiken wird sichergestellt, dass das Wissen bezüglich der vorhandenen Risiken in der Bundesverwaltung auf dem aktuellsten Stand gehalten wird. Ziel ist es, einerseits Veränderungen im Umfeld zu erkennen, die zu einer Neueinschätzung von bereits erfassten Risiken führen. Andererseits geht es auch darum, neu entstehende Risiken frühzeitig zu erkennen.

Bereits erfasste Risiken müssen zusätzlich zum jährlichen Risikomanagementprozess laufend überwacht werden, damit bei einer Verschlechterung der Situation frühzeitig eingegriffen werden kann.

Im Bereich der Früherkennung von *neuen Risiken* ist die Bundesverwaltung auf wachsame Führungskräfte und Mitarbeiter angewiesen. Diese müssen interne und externe Veränderungen verfolgen und zeitgerecht erkennen. Dazu sind sie mit entsprechenden externen Know-how-Trägern vernetzt.

In der Bundesverwaltung findet die Überwachung der Risiken in erster Linie durch die Risikoeigner statt, die sich im Rahmen ihres Pflichtenheftes auch mit den Risiken in ihrem Aufgabenbereich befassen müssen.

3.6.2 Massnahmen-Überwachung

Die Umsetzung von Massnahmen zur Risikoreduktion muss überwacht werden. Dies ist Aufgabe des Risikoeigners, der die Verantwortung für das Risiko trägt. Der Massnahmenverantwortliche setzt die beschlossene Massnahme um und rapportiert dem Risikoeigner über den Fortschritt und allfällige Probleme bei der Massnahmenumsetzung. Beschlossene Massnahmen fliessen zudem in die Planungs- und Reporting-Instrumente der Bundesverwaltung ein.

Prozessschritt Risiko- und Massnahmenüberwachung:
Vorgabe EFV:
- Die Überwachung der Risiken und der Massnahmen erfolgt durch den Risikoeigner.

4 Reporting

Das Reporting der analysierten Risiken ist ein wichtiger Output des Risikomanagement-Prozesses. Im Risikoreporting werden die Ergebnisse aus dem Risikomanagement vorgestellt. Diese sollen die Entscheidfindung der Führung im Umgang mit den Risiken unterstützen.

4.1 Inhalt des Risikoreportings

Das Risikoreporting muss mindestens die folgenden Elemente enthalten:

- Eine *Riskmap*, welche die Risikolandschaft der OE darstellt und die Risiken einander gegenüberstellt;
- Die *Entwicklung* der Risiken gegenüber dem letzten Risikoreporting;
- Eine *Massnahmenliste*, die insbesondere über den Stand der Umsetzung bei beschlossenen Massnahmen und die Entscheidungsgrundlagen bei neuen, möglichen Massnahmen Auskunft gibt;
- wichtige *Wechselwirkungen* zwischen erfassten Risiken (vgl. Ziff. 4.5).

Risikoreporting:
Vorgabe EFV:

- Die Risikoreportings in der Bundesverwaltung umfassen mindestens eine Riskmap, die Entwicklung der Risiken, wichtige Wechselwirkungen zwischen Risiken und eine Massnahmenliste mit den möglichen und den sich in Umsetzung befindlichen Massnahmen.

4.2 Reporting-Grundsätze

Ein verständliches, übersichtliches und aktuelles Risikoreporting hilft den Entscheidungsträgern, die relevanten Informationen schnell zu erkennen und optimale Entscheidungen bezüglich den Risiken zu treffen. Einige Grundsätze dazu:

- Eine geeignete Anzahl Risiken auswählen (Konzentration auf Risiken, die von den Adressaten beeinflusst werden können; vgl. Ziff. 4.4);
- Kurze, prägnante und für Dritte verständliche Beschreibung der Risiken (nicht zu wenig und nicht zu viel Informationen, kein «Fachchinesisch»).

4.3 Aggregation von Querschnittsrisiken

In grossen Organisationen wie der Bundesverwaltung kommt es regelmässig vor, dass in verschiedenen Departementen oder VE die *gleichen oder ähnliche* Risiken identifiziert werden oder dass ein identifiziertes Risiko mehrere OE betrifft. Beispielsweise tangiert der Ausfall eines zentralen EDV-Systems oft mehrere VE. Bei solchen sogenannten Querschnittsrisiken kann es Sinn machen, sie (allenfalls nur zum Teil) zentral zu bewirtschaften und im Reporting auf übergeordneter Stufen (Departement bzw. Bundesrat) zu aggregieren. Bei der Aggregation eines Risikos wird dieses auf der übergeordneten Stufe analysiert, Wechselwirkungen werden aufgezeigt. Die Eintrittswahrscheinlichkeit und die Auswirkungen (des «credible-worst-case»-Szenarios) werden neu eingeschätzt, wobei die Einschätzungen und Annahmen der untergeordneten Stufen mitberücksichtigt werden.

Die nachfolgenden Grundsätze der Risikoaggregation sollen ein gemeinsames Verständnis und ein möglichst einheitliches Vorgehen bei der Risikoaggregation in der Bundesverwaltung sicherstellen.[26]

[26] Vgl. auch Anhang 10, wo für einige konkrete Querschnittsrisiken die Zusammenhänge und die bundesweiten Strukturen aufgezeigt werden.

4.3.1 Aggregationsentscheid[27]

Eine Aggregation von Risiken soll nur erfolgen, wenn sich daraus ein Mehrwert ergibt, beispielsweise:

- Die Gesamtbedeutung eines Risikos bzw. ein Handlungsbedarf wird erst bei der Aggregation der Teilrisiken auf übergeordneter Stufe erkennbar.
  Beispiel: Die gesamten negativen Auswirkungen eines IT-Serverausfalls sind erst erkennbar, wenn die Auswirkungen der ausfallenden Anwendungen in den einzelnen VE *summiert* betrachtet werden.
- Das Risiko kann mit zentral gesteuerten Massnahmen effizienter oder kostengünstiger bewirtschaftet werden (Nutzung von Skaleneffekten).
  Beispiel: Es ist weniger teuer, eine Sensibilisierungskampagne zum sicheren Umgang mit Passwörtern bundesweit durchzuführen, als in jeder VE einzeln.
- Die für die Reduktion eines Risikos zur Verfügung stehenden Mittel können durch die Priorisierung der Minimierungsmassnahmen im Rahmen einer Aggregation effizienter zugeteilt werden.
  Beispiel: Die für die Verbesserung der Erdbebensicherheit budgetierten Mittel werden dann am wirkungsvollsten eingesetzt, wenn die Erdbebensicherheit *aller* Bundesgebäude geprüft, somit eine aggregierte Sichtweise eingenommen und eine Priorisierung vorgenommen wurde.
- Die Aggregation auf übergeordneter Stufe fördert die Identifikation und das Verständnis von Wechselwirkungen und Schnittstellen.
  Beispiel: Die Wechselwirkungen zwischen der Unternehmenssteuerreform III (ESTV), den Auswirkungen auf den Bundeshaushalt (EFV) und den Beziehungen mit der EU (SIF) können auf Stufe Departement analysiert und bewirtschaftet werden.

Es muss hier davor gewarnt werden, dass eine Aggregation unter Umständen zu einer Trivialisierung der Risiken führen kann. Eine Aggregation sollte nicht durchgeführt werden, nur um auf übergeordneter Hierarchiestufe eine bessere, thematisch gruppierte Übersicht zu erreichen. Es besteht dabei nämlich die Gefahr, dass bei der Aggregation relevante Risikoinformationen verloren gehen und dass das zusammengefasste Risiko so allgemein formuliert werden muss, dass die Gefährdung und der Handlungsbedarf nicht mehr ersichtlich sind.

- *Negativbeispiele:* Zusammenfassung eines Flugzeugabsturzes, einer Zugsentgleisung und eines Tunnelbrandes als «Grossunfälle»; Know-How-Verluste, Korruption, fehlende Arbeitsmotivation und Veruntreuung als «Personalrisiken»; Zeitverzögerungen in mehreren, voneinander unabhängigen Projekten als «Zeitverzögerung Projekte».

4.3.2 Zuständigkeit für die Aggregation[28]

Die Verantwortung bzw. Federführung *für die Aggregation* eines Querschnittsrisikos muss im Rahmen des Risikomanagementprozesses geklärt werden. Davon unabhängig ist die Verantwortung *für die Risikobewirtschaftung:* Diese ergibt sich aufgrund der Aufgaben der OE und liegt bei Querschnittsrisiken häufig auf mehreren Ebenen oder bei mehreren OE.

Grundsätzlich gibt es zwei Zuordnungsmöglichkeiten:

- Eine VE, eine interdepartementale Arbeitsgruppe (oder allenfalls eine Projektleitung) hat bereits einen konkreten ***Auftrag zur zentralen Steuerung und Bewirtschaftung***

[27] Die Koordinationsstelle Risikomanagement Bund führt einen Katalog mit wichtigen Querschnittsrisiken der Bundesverwaltung, die aggregiert werden sollen.
[28] Die Koordinationsstelle Risikomanagement Bund führt eine Liste, in der die Federführung für die Aggregation von wichtigen Querschnittsrisiken der Bundesverwaltung aufgeführt wird.

eines Querschnittsrisikos für die gesamte Bundesverwaltung (Gesetz, Organisationsverordnung, Beauftragung z. B. durch den Bundesrat etc.). Sie übernimmt die Federführung für eine aggregierte Risikobetrachtung und zieht die Informationen aus den betroffenen VE bei. Die Koordinationsstelle Risikomanagement Bund bzw. die Risikomanager unterstützen sie in methodischer Hinsicht.

- Wenn ***keine zentrale Steuerung*** existiert, erfolgt die Federführung und Steuerung für die Risikoaggregation durch die betroffenen Risikomanager bzw. durch die Koordinationsstelle Risikomanagement Bund. Diese ziehen die notwendigen Fachexperten und die für die Risikobewirtschaftung zuständigen OE bei.

4.3.3 Klärung der Verantwortlichkeiten

Bei der Bewirtschaftung von Querschnittsrisiken, insbesondere bei der Umsetzung von Risikominimierungsmassnahmen, sind meistens mehrere VE zu beteiligen (z. B. Abwehrmassnahmen gegen Cyberattacken). Aus den Aufgaben der betroffenen VE lässt sich in der Regel ableiten, bei welcher OE die Verantwortung für einen Teilaspekt der Risikobewirtschaftung am sinnvollsten anzusiedeln ist (Identifikation, Bewertung, Massnahmen [Evaluation, Entscheid, Umsetzung], Überwachung). Die Schnittstellen in der Zusammenarbeit müssen geklärt und die Verantwortlichkeiten festgelegt werden. Nur so lassen sich Doppelspurigkeiten oder Lücken in der Bewirtschaftung von Querschnittsrisiken vermeiden.

4.3.4 Reporting

Querschnittsrisiken sollen grundsätzlich sowohl auf der Stufe VE (falls für die VE relevant) als auch (aggregiert) auf übergeordneter Stufe in die Risikoberichterstattung einfliessen.[29]

4.3.5 Informationsaustausch

Ein steter Informationsaustausch zwischen Risikomanagern, Risikocoaches und Risikoeignern, die sich mit bestimmten Querschnittsrisiken befassen, ist von grosser Bedeutung.[30] Erfahrungen können ausgetauscht und neue Ideen im Umgang mit dem Querschnittsrisiko entwickelt werden.

Grundsätze Risikoaggregation:
Vorgaben EFV:

- Bei Querschnittsrisiken ist jeweils zu prüfen, ob und auf welcher Stufe (VE, Departement, Bund) eine Aggregation sinnvoll oder gar notwendig ist.
- Die Zuständigkeit bzw. Federführung für die Risikoaggregation ist festzulegen.
- Die Aufgaben und Verantwortlichkeiten der Akteure (Identifikation, Analyse, Bewertung, Massnahmen, Überwachung) sind zu klären bzw. festzulegen. Fehlende Informationen für eine aggregierte Risikobetrachtung sind zu beschaffen.
- Für die Risikoberichterstattung ist das aggregierte Risiko übersichtlich, verständlich und möglichst umfassend darzustellen.
- Der Informationsaustausch zwischen allen Akteuren ist aktiv zu fördern.

[29] Bei einer Aggregation von Risiken auf übergeordneter Stufe erscheinen die aggregierten Quellrisiken nicht auf der Riskmap, wenn im R2C die Aggregation mit der Funktion «aggregiertes Risiko» durchgeführt wird.
[30] Die Koordinationsstelle Risikomanagement Bund unterstützt den Informations- und Erfahrungsaustausch zwischen den VE und Departementen mit Veranstaltungen, Informationsnotizen etc.

4.4 Auswahl von Risiken

Bei Vorhandensein vieler Risiken ist es im Rahmen des Reportings sinnvoll, sich auf wenige und für die Entscheidungsträger relevante Risiken zu konzentrieren. Die Konzentration auf diese Risiken erleichtert die Lesbarkeit einer Riskmap und ermöglicht es den Führungskräften, sich auf die Bewirtschaftung der für sie wichtigsten Risiken zu konzentrieren. Informationsdichte: Je höher die Hierarchiestufe, desto verdichteter muss die Information dargestellt werden.

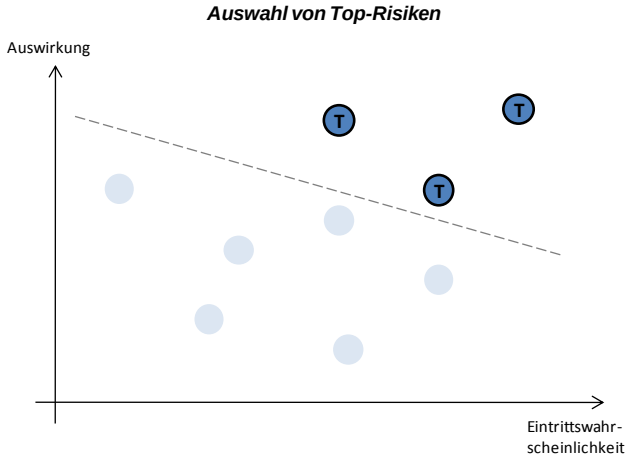


Abbildung 12: Auswahl von Top-Risiken

In der Bundesverwaltung wird mit den folgenden Regeln ein stufengerechtes Reporting sichergestellt:

Auf Stufe der VE werden im Risikomanagementprozess die vorhandenen Risiken erfasst, analysiert und bewertet. Gleichzeitig erfolgt der gleiche Prozess auch im Generalsekretariat der Departemente, das sich mit Risiken auf Stufe Departement (Top-Down-Sicht) auseinandersetzt. Eine Auswahl dieser Risiken wird an die Leitung der VE rapportiert. In den Richtlinien werden keine Vorgaben gemacht, wie innerhalb einer VE die Risiken für die Leitung konsolidiert werden. Die Koordinationsstelle EFV empfiehlt aber, dass in Absprache mit dem Leiter der VE eine Reportingschwelle VE und/oder eine grobe Anzahl Toprisiken festgelegt werden.

Jede VE meldet danach ihre drei grössten Risiken an den Risikomanager des Departements. Falls mehr als drei Risiken die Reportingschwelle des Departements überschreiten, werden auch diese weitergemeldet. Die Reportingschwelle auf Stufe Departement wird durch die Leitung des Departements definiert und muss mit den Vorgaben auf Stufe Bundesrat abgestimmt sein. Risiken, die nicht an das Departement gemeldet werden gelten als sogenannte *Bereichsrisiken*. Die aus den VE an das Departement gemeldeten Risiken sind *Departementsrisiken*.

Für das Bundesratsreporting meldet jedes Departement und die BK der Koordinationsstelle EFV seine/ihre grössten drei Risiken. Die Leitung des Departements / der BK definiert die drei Toprisiken ihrer OE. Zusätzlich müssen weitere Risiken gemeldet werden, wenn diese eine sehr hohe Auswirkung haben oder eine hohe Auswirkung und wahrscheinlich oder sehr wahrscheinlich sind (33%–100% Eintrittswahrscheinlichkeit). Die von jedem Departement und der BK gemeldeten Risiken werden *Kernrisiken* genannt. Diese Risiken werden durch die Koordinationsstelle EFV geprüft: Es findet eine erste Plausibilisierung, ein Quervergleich und eine erste Harmonisierung der Risiken statt. In einem Gespräch mit dem Generalsekretär je Departement können Rückfragen gestellt werden und die Risiken allenfalls angepasst

werden. Die überarbeiteten Risiken werden danach der GSK vorgelegt. Diese prüft die Risiken auf ihre Vollständigkeit und aggregiert allfällige Querschnittsrisiken. Danach werden die wichtigsten Risiken für das Reporting zuhanden des Bundesrates ausgewählt. Als Richtgrösse gelten 10–15 Risiken, die dem Bundesrat unterbreitet werden sollen. Diese gelten als sogenannte *Bundesratsrisiken.*

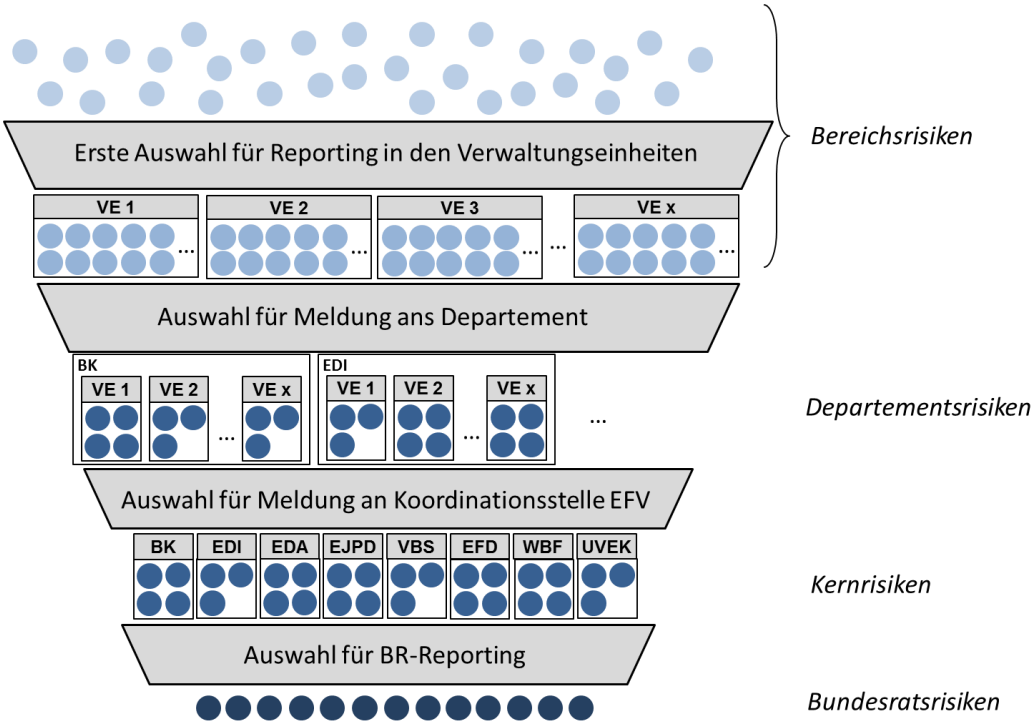


Abbildung 13: Auswahl von Risiken in der Bundesverwaltung

4.5 Wechselwirkungen

4.5.1 Organisatorischer Umgang mit Wechselwirkungen

Auf *Stufe Bundesrat* übernimmt die Generalsekretärenkonferenz die Aufgabe, die aus den Departementen und der BK gemeldeten Risiken auf Wechselwirkungen hin zu prüfen. Die Koordinationsstelle EFV initiiert und begleitet die dazu notwendigen interdepartementalen Abstimmungen.

Auf *Stufe Departement* koordiniert der Risikomanager die notwendigen Abstimmungen zur Analyse und Bewirtschaftung von verwaltungseinheitsübergreifenden Wechselwirkungen innerhalb des Departements.

Wenn in einer VE ein Risiko Wechselwirkungen mit einem Risiko einer VE aus einem *anderen* Departement / der BK aufweist, initiiert und begleitet die Koordinationsstelle EFV die Abstimmung zwischen diesen zwei VE.

4.5.2 Abbildung von Wechselwirkungen

Für eine quantifizierte Aggregation aller Risiken ist die genaue Definition des Wirkungsmechanismus erforderlich. Aber auch bei einer qualitativen Betrachtung (wie sie in der Bundesverwaltung auf Stufe Departement / BK und Bundesrat stattfindet) ist die Analyse und das Verständnis von allfälligen Wechselwirkungen wichtig, um:

- das Gefahrenpotential von verketteten Risiken zu erkennen.
- Ansätze zu erarbeiten, um diese Verkettungen allenfalls aufzubrechen.

Wechselwirkungen mit anderen Risiken werden in der Risikobeschreibung *verbal* erfasst und erläutert. Allenfalls können sie grafisch dargestellt werden.

Risikoreporting:
Vorgaben EFV:
- Die VE melden dem Departement alle Risiken, die über dem vom Departement definierten Schwellenwert eingestuft sind, mindestens aber ihre drei grössten.
- Die Departemente und die BK melden der Koordinationsstelle EFV alle Risiken, die über dem Schwellenwert Bund eingestuft sind (Risiken mit «sehr hoher» Auswirkung sowie Risiken mit «hoher» Auswirkung, sofern ihre Eintrittswahrscheinlichkeit mit «wahrscheinlich» oder «sehr wahrscheinlich» bewertet wird), mindestens aber ihre drei grössten.
- Wechselwirkungen zwischen Risiken werden analysiert und im Risikoreporting verbal oder grafisch erläutert.
- Querschnittsrisiken werden bei Bedarf auf den übergeordneten Hierarchiestufen aggregiert.

5 Kommunikation

Die Informationsflüsse und die Kommunikation zwischen den verschiedenen Akteuren im Risikomanagement sind wichtig und müssen, je nach Bedarf, in jeder Phase des Risikomanagementprozesses erfolgen (vgl. Ziff. 3.1). Eine gut aufgestellte interne und externe Kommunikation ist notwendig und nützlich, um
- die Risiken unter Berücksichtigung mehrerer Aspekte (aus verschiedenen Bereichen) und mit dem besten vorhandenen Fachwissen zu analysieren;
- sicherzustellen, dass die Interessen, Informationsbedürfnisse und Wahrnehmungen aller Anspruchsgruppen berücksichtigt werden und dadurch das Vertrauen in das Risikomanagement gestärkt wird;
- sicherzustellen, dass angemessen und zeitgerecht auf Veränderungen der Risikosituation reagiert werden kann.

Die Risikokommunikation in ausserordentlichen Lagen (Notfall- und Krisensituationen) wird durch die Bundeskanzlei organisiert und gesteuert und somit im folgenden Abschnitt nicht beschrieben.

Bereits in Ziffer 3.1 werden die Informationsflüsse zwischen den einzelnen Akteuren im Risikomanagementprozess detailliert erläutert. In Ziffer 5.1 werden weitere Elemente der internen Risikokommunikation beschrieben. Ziffer 5.2 befasst sich mit der Risikokommunikation der Bundesverwaltung nach aussen. In Ziffer 5.3 wird auf das Öffentlichkeitsprinzip, der Klassifizierung und der Archivierung von Informationen im Risikomanagement eingegangen.

5.1 Interne Kommunikation und Schulungen

Im Rahmen von Schulungen, Veranstaltungen und internen Informationskanälen wird sichergestellt, dass innerhalb der Bundesverwaltung die Mitarbeitenden bezüglich dem Thema Risikomanagement ausgebildet und sensibilisiert werden. Dadurch soll die vorhandene Risikokultur verbessert, ein Austausch von Wissen im Bereich Risikomanagement ermöglicht und das Wissen zum Risikomanagement erhöht werden.

5.1.1 Schulungen

Folgende Kurse im Bereich Risikomanagement werden in der Bundesverwaltung regelmässig angeboten:

Schulung	Dauer	Häufigkeit	Zielgruppe
Risikomanagement für Topkader	½ Tag	ca. 2 Mal im Jahr	Risikoeigner
Grundlagen Risikomanagement	1Tag	ca. 2 Mal im Jahr	Interessierte Personen (BCM-Beauftragte, Juristen, Projektmanager etc.)
Kurs «Risiken verstehen und bewältigen»	3 Tage	ca. 2 Mal im Jahr	Risikomanager und Risikocoaches
Kurs Risk-to-Chance (R2C)	½ Tag	ca. 2-3 Mal im Jahr	Risikomanager und Risikocoaches
Refresherkurs	1 Tag	ca. 2 Mal im Jahr	Ausgebildete Risikomanager und Risikocoaches

5.1.1.1 Kurs «Risiken verstehen und bewältigen»

In diesem Kurs werden die Grundlagen des Risikomanagements in der Bundesverwaltung vorgestellt. Die Teilnehmer lernen den Risikomanagementprozess, Methoden zur Risikobewertung und den Aufbau eines Risikomanagementsystems kennen und werden befähigt, dies in ihrer Organisationseinheit umzusetzen. Die wichtigsten Elemente des vorliegenden Handbuchs werden im Kurs behandelt und erläutert. Der Kurs ist für Risikomanager und Risikocoaches obligatorisch.

5.1.1.2 Schulung R2C

Die in der Bundesverwaltung verwendete Software zur Bewirtschaftung der Risiken heisst Risk-to-Chance (R2C) und wird von der Firma Schleupen AG aus Deutschland angeboten[31]. In einem ausführlichen Benutzerhandbuch werden alle Funktionalitäten der Software erläutert.[32] Innerhalb der Bundesverwaltung betreut die Koordinationsstelle EFV die Anwendung R2C und ist erste Ansprechpartnerin bei Fragen, Problemen und Erteilung von Berechtigungen. Grundsätzlich werden die Risiken im System durch die jeweiligen Risikocoaches der VE und Risikomanager der Departemente / der BK bewirtschaftet. Diese haben jeweils nur Zugriff auf die Risiken der eigenen Organisationseinheit. Zudem besteht die Möglichkeit, für einzelne Mitarbeiter Einsichtsberechtigungen zu erteilen.

In einem halbtägigen Kurs werden der Aufbau, die Navigation und die wichtigsten Funktionen der Software Risk-to-Chance (R2C) vorgestellt. Die Teilnehmer können im Kurs an einem eigenen PC die Benützung der Software üben und direkt Fragen stellen.
Der Kurs wird von der Koordinationsstelle EFV durchgeführt. Da die Software R2C für die Bewirtschaftung der Risiken im Bund verwendet wird, ist für Risikomanager und Risikocoaches die Teilnahme am Kurs obligatorisch.

5.1.1.3 Ausbildungskurs für Kader (Risikoeigner)

Mit diesem Kurs sollen Risikoeigner in der Bundesverwaltung bzgl. ihrer Verantwortung im Umgang mit Risiken geschult und sensibilisiert werden.

[31] Diese bietet auch einen technischen Support an.
[32] http://intranet.efd.admin.ch/efv/fachinfo/04322/04750/index.html?lang=de

Vorgabe EFV:

- Die Kurse R2C-Schulung und «Risiken verstehen und bewältigen» sind grundsätzlich für alle Risikomanager und Risikocoaches obligatorisch.

5.1.2 Veranstaltungen

Netzwerk Risikomanagement

Der Verein Netzwerk Risikomanagement schafft für die im Risikomanagementprozess involvierten Personen eine Plattform für berufliche Kontakte, Erfahrungsaustausch und Weiterbildung. Angeboten werden praxisbezogene Veranstaltungen und Publikationen. Es ist geplant, jährlich eine bis zwei Veranstaltungen zu einem konkreten Risikomanagement-Thema durchzuführen. Der Teilnehmerkreis umfasst primär alle in der Bundesverwaltung interessierte Personen, die einen Bezug zum Risikomanagement haben und weitere am Risikomanagement interessierte Personen.

Innerhalb der Departemente / der BK und der VE finden zudem weitere, meist spezifischere Veranstaltungen zu konkreten Risikothemen statt.

Ein Austausch des Risikomanagementwissens innerhalb der Bundesverwaltung ist erwünscht und wird durch die Koordinationsstelle EFV gesteuert und unterstützt.

5.1.3 Interne Informationskanäle

5.1.3.1 Intranetbereich Risikomanagement

Ein speziell für die Risikomanager und Risikocoaches erstellter und geschützter Bereich im Intranet des EFD ermöglicht den unkomplizierten fachlichen Austausch unter den Risikomanagern und -coaches. Hier werden die Weisungen, Richtlinien und das Handbuch zum Risikomanagement Bund, fachlich-methodische Unterlagen zum Risikomanagement und spezifische Hilfsmittel und Instrumente zur Umsetzung des Risikomanagementprozesses abgelegt.

5.1.3.2 Newsletter Risikomanagement

Ein Newsletter der Koordinationsstelle EFV an die Risikomanager und Risikocoaches und weitere Anspruchsgruppen berichtet periodisch über aktuelle Themen und Entwicklungen im Risikomanagement.

5.2 Externe Kommunikation

Der Bundesrat nimmt zuhanden der Öffentlichkeit zum Thema Risikomanagement Bund Stellung.

5.2.1 Geschäftsbericht

Der Bundesrat erstattet der Bundesversammlung jährlich einen Bericht über seine Geschäftsführung. Dieser Bericht ist öffentlich und auf der Homepage der Bundeskanzlei aufgeschaltet[33]. Im Band I «Schwerpunkte der Geschäftsführung des Bundesrates» findet sich jeweils ein Beitrag zum Thema Risikomanagement Bund. Darin werden in erster Linie konzep-

[33] http://www.bk.admin.ch/dokumentation/publikationen/00290/00929/index.html?lang=de

tionell-organisatorische Neuerungen im Risikomanagement des Bundes dargelegt. Auf einzelne Risiken des Bundes wird nur in sehr allgemeiner Form eingegangen.

5.2.2 Staatsrechnung und Voranschlag (Budget)

Auch die Staatsrechnungen[34] und die Voranschläge[35] sind öffentlich zugängliche Dokumente. Sie enthalten verschiedene Informationen aus dem Risikomanagement.

1. Im «Anhang zur Jahresrechnung» (Staatsrechnung Band 1) und im Voranschlag findet sich jeweils ein *allgemeines Kapitel* «Risikomanagement und Risikosituation». Dieses enthält Informationen zum Umgang mit Risiken, zu den Instrumenten und den Massnahmen des Risikomanagements, zur allgemeinen Risikosituation des Bundes und zur Offenlegung der Risiken. Aus Gründen der Vertraulichkeit wird auf eine genaue Bezeichnung und Detailangaben zu einzelnen Risiken verzichtet, soweit sie nicht bilanziert sind oder in den Eventualverbindlichkeiten offen gelegt werden.
2. Die Umsetzungskosten der im Rahmen des Risikomanagements beschlossenen und durchzuführenden *Massnahmen* sind im Budgetierungsprozess zu berücksichtigen.
3. Die rechtlichen Voraussetzungen für die Behandlung von Risiken im Voranschlag und in der Rechnung sind im Finanzhaushaltsgesetz[36] und in der Finanzhaushaltsverordnung[37] festgelegt (siehe Übersicht in Anhang 6). Dabei sind die einschlägigen Bestimmungen gemäss den «Richtlinien und Weisungen zur Haushaltführung Bund» zu beachten.[38]

Der allgemeine Abschnitt zum Risikomanagement im Anhang der Jahresrechnung wird von der Koordinationsstelle EFV erstellt. Für die Aufnahme von beschlossenen Massnahmen und den aus dem Gesetz vorgeschriebenen Verpflichtungen (Rückstellungen und Eventualverbindlichkeiten) in den Voranschlag und der Staatsrechnung ist in erster Linie der entsprechende Risikoeigner bzw. die zuständige VE verantwortlich.

5.2.3 Stellungnahme des Bundesrates zu parlamentarischen Berichten bezüglich Risikomanagement

Die Geschäftsprüfungskommissionen (GPK) und die Finanzdelegation der eidgenössischen Räte begleiten das Risikomanagement Bund seit Jahren sehr eng. Sie berichten über ihre Tätigkeit im Bereich Risikomanagement Bund im Rahmen ihrer Jahresberichte oder in separaten Berichten. Diese werden jeweils im Bundesblatt[39] publiziert, meistens zusammen mit der entsprechenden Stellungnahme des Bundesrates. Diese parlamentarischen Berichte, wie auch die publizierten Stellungnahmen des Bundesrates, befassen sich nicht mit einzelnen Risiken des Bundes.[40]

---

[34] http://www.efv.admin.ch/d/dokumentation/finanzberichterstattung/staatsrechnungen.php
[35] http://www.efv.admin.ch/d/dokumentation/finanzberichterstattung/budget.php
[36] FHG Art 49 Abs. 3
[37] FHV Art. 3 Bst. b und d; Art. 56 Abs. 2
[38] http://intranet.accounting.admin.ch/ ; zu beachten sind insbesondere die Handbuchkapitel *5.3.4 Rückstellungen* und *10.2 Eventualforderungen und -verbindlichkeiten*.
[39] http://www.admin.ch/ch/d/ff/index.html
[40] Die Risikoberichterstattung an den Bundesrat wird in der Regel im April im Rahmen einer Arbeitsgruppe der GPK behandelt.

5.3 Klassifizierung, Öffentlichkeitsprinzip und Archivierung

5.3.1 Klassifizierung von Informationen im Risikomanagement

Die Klassifizierung und die Bearbeitung von schützenswerten Informationen und Dokumenten des Bundes sind in der Informationsschutzverordnung[41] geregelt. Es wird zwischen geheimen, vertraulichen, internen und offenen Informationen unterschieden. Klassifizierte Informationen dürfen nur jenen Personen bekannt gegeben oder zugänglich gemacht werden, die davon Kenntnis haben müssen. Im Risikomanagement des Bundes sind die Informationen, Daten und Datenträger je nach ihrem Schutzbedarf durch den Verfasser (VE, Departement / BK oder Koordinationsstelle Risikomanagement EFV) folgendermassen zu klassifizieren:

Informationen / Dokumente	*Schutzbedarf / Klassifizierung*
Einzelrisiko-Reports	VERTRAULICH
Risikoreportings (VE, Departement / BK, Bundesrat)	VERTRAULICH
Daten innerhalb der Software R2C	VERTRAULICH
Bewertungsmatrix	INTERN
Risikorichtlinien EFV	nicht klassifiziert (offen)
Handbuch Risikomanagement Bund	nicht klassifiziert (offen)

Vorgabe EFV:
- Die im Risikomanagement Bund involvierten Personen halten die Informationsschutzvorschriften gemäss ISchV ein.

5.3.2 Öffentlichkeitsprinzip

Gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung[42] hat grundsätzlich jede Person das Recht, «amtliche Dokumente[43] einzusehen und von den Behörden Auskünfte über den Inhalt amtlicher Dokumente zu erhalten» (Art. 6 Abs. 1 BGÖ). Der Zugang zu amtlichen Dokumenten wird jedoch eingeschränkt, aufgeschoben oder verweigert, wenn eine Ausnahme nach Artikel 7 oder 8 BGÖ vorliegt. Nach Ansicht der EFV müssen Einsichtsgesuche betreffend vertrauliche Dokumente aus dem Risikomanagement Bund gestützt auf diese Bestimmungen abgewiesen werden.[44] Bis heute wurde noch nie ein solches BGÖ-Einsichtsgesuch gerichtlich beurteilt.

5.3.3 Archivierung

Die Unterlagen, die im Rahmen des Risikomanagements Bund erstellt (oder empfangen) worden sind, unterstehen den Bestimmungen des Bundesgesetzes über die Archivierung[45]. Die Departemente, die BK und die VE sind selber für die Archivierung ihrer Unterlagen verantwortlich.

Zudem werden die einzelnen Risiken innerhalb der Risikomanagement-Applikation Risk-to-Chance (R2C) *elektronisch* gespeichert und archiviert. Die Risiken werden mindestens einmal jährlich erfasst bzw. aktualisiert und danach innerhalb des R2C historisiert. Bei *eingetre-*

[41] ISchV; SR *510.411*
[42] Öffentlichkeitsgesetz, BGÖ; SR *152.3*
[43] Als amtliches Dokument gilt jede Information, die auf einem beliebigen Informationsträger aufgezeichnet ist und die Erfüllung einer öffentlichen Aufgabe betrifft (Art. 5 Abs. 1 BGÖ).
[44] Vgl. Anhang 5 (Beispiel einer Einsichtsverweigerung)
[45] Archivierungsgesetz, BGA; SR *152.1*

tenen Risiken werden zusätzlich die erlittenen Schäden und die dazugewonnenen Erkenntnisse im R2C festgehalten. *Erledigte* Risiken werden aus Gründen der Nachvollziehbarkeit im R2C nicht gelöscht; ihr Status ist auf «erledigt» zu setzen.

6 Schnittstellen

Im Folgenden werden Organisationseinheiten, Projekte und Funktionen innerhalb der Bundesverwaltung beschrieben, die eine Schnittstelle zum Risikomanagement aufweisen. Das Ziel ist, die Aufgaben der jeweiligen Funktion oder Organisation kurz zu erläutern, von den Aufgaben im Risikomanagement abzugrenzen und die Schnittstellen und Informationsflüsse festzulegen. Dies soll zu einem effizienten Risikomanagement ohne Doppelspurigkeiten und Reibungsverlusten beitragen.

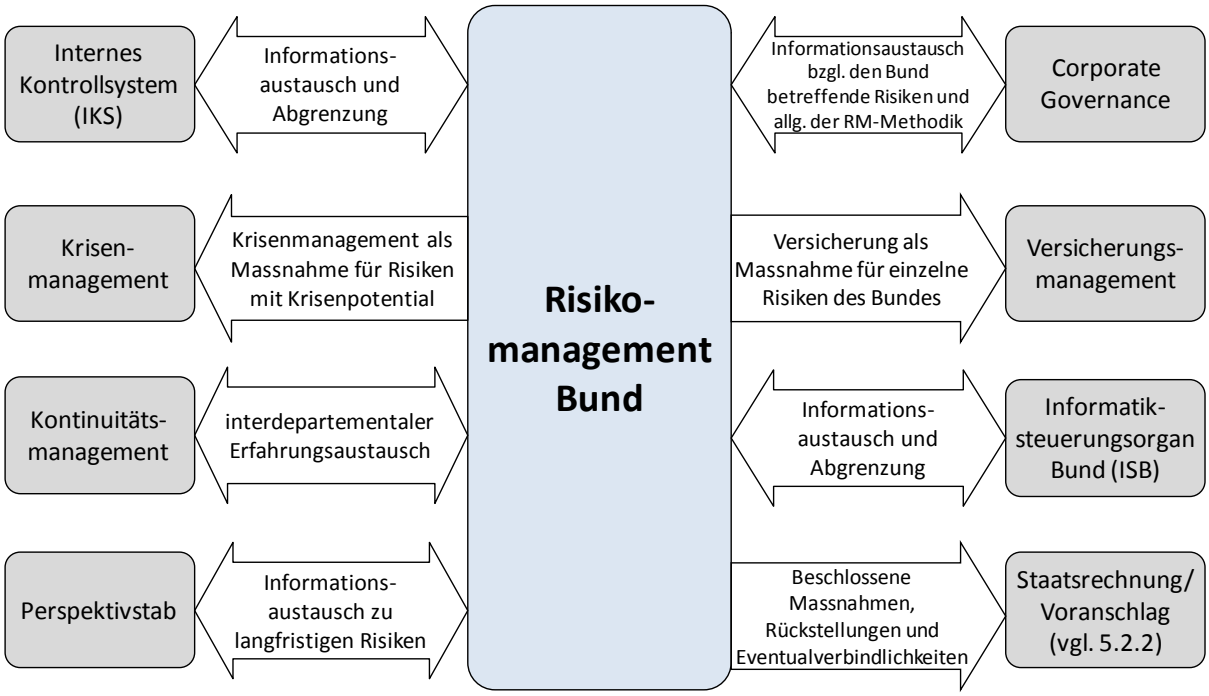


Abbildung 14: Schnittstellen zum Risikomanagement (nicht abschliessend)

6.1 Internes Kontrollsystem (IKS)

Das Interne Kontrollsystem (Art. 39 FHG, Art. 36 FHV) identifiziert operative finanzbezogene Risiken. Es beschreibt und bewertet die identifizierten Risiken und legt risikominimierende regulatorische, organisatorische und technische Kontrollmassnahmen fest. Es erfolgt eine periodische Überprüfung sowohl der identifizierten und bewerteten Risiken als auch der Wirksamkeit der risikominimierenden Kontrollen. Das IKS unterscheidet zwischen automatisierten (beispielsweise Berechtigungen und Validierungen) und manuellen (beispielsweise Verifizierung/Plausibilisierung, Vier-Augen-Prinzip) Kontrollen, wobei wenn möglich automatisierte Kontrollen einzuführen sind.

Im Gegensatz zum breit angelegten Risikomanagement konzentriert sich das IKS auf die Identifikation von operativen Risiken der finanzrelevanten Geschäftsprozesse und auf die Beschreibung und Umsetzung geeigneter Kontrollmassnahmen zur Minimierung dieser Risiken. Das IKS ist demnach Teil des Risikomanagements der Bundesverwaltung.

Abbildung 15: IKS und Risikomanagement

Schnittstellen zum Risikomanagement:
Die Identifikation und Bewertung von operativen Risiken der finanzrelevanten Geschäftsprozesse und die Erarbeitung von Kontrollmassnahmen fällt theoretisch in den Aufgabenbereich sowohl des Risikocoaches als auch des IKS-Beauftragten. Im Sinne einer optimalen Arbeitsteilung konzentriert sich der Risikocoach im Risikomanagement-Prozess auf die Identifikation aller anderen Risiken der VE, ergänzt seine Risikoliste aber mit den relevanten im IKS-Prozess identifizierten Risiken.

Notwendiger Informationsaustausch:
Auf Stufe VE soll ein regelmässiger Austausch zwischen dem Risikocoach und dem IKS-Beauftragten stattfinden. Dabei wird analysiert,

- ob die identifizierten Risiken aus dem Risikomanagement Anpassungen im IKS bzw. neue Massnahmen im Sinne von Kontrollen erfordern.
- ob im IKS-Prozess erkannte Risiken im Risikomanagement zu erfassen sind und einer Berichterstattung bedürfen.

6.2 Notfall- und Krisenmanagement

Ein zweckmässiges Notfall- und Krisenmanagement ist Teil des Risikomanagements[46] und zuständig für die Bewältigung von gravierenden Risiken bei deren Eintritt. Bei Risiken mit hohen Auswirkungen ist es wichtig, über Organe, Einrichtungen und Prozesse zu verfügen, die einen Schadenplatz so schnell als möglich beheben (Notfallmanagement) oder die Reputation, den Handlungsspielraum oder die Existenz der betroffenen Organisation verteidigen (Krisenmanagement) [47]. Zusätzlich müssen, je nach Dauer der Wiederherstellungsphase, die Kernprozesse der betroffenen Organisation aufrecht erhalten werden (Kontinuitätsmanagement[48]). In diesem Sinn sind Notfall-, Krisen- und Kontinuitätsmanagement für Massnahmen

[46] Ziff. 4 Abs. 6 der Weisungen des Bundesrates vom 24.09.2010 über die Risikopolitik des Bundes (BBl *2010* 6549) (hiernach: Weisungen)
[47] Siehe Definitionen «Notfall» und «Krise» in Anhang 1.
[48] Vorkehrungen zum Kontinuitätsmanagement werden auch im Vorfeld erarbeitet und sind in diesem Sinn auch Bewältigungsoptionen des Risikomanagements (vgl. Ziff. 6.3).

zuständig, die zur Bewältigung von Schaden und zur Linderung der Konsequenzen bei eingetroffenen Risiken beitragen. Die Beschlussfassung über solche Massnahmen liegt grundsätzlich in der Verantwortung der Linie. Das Risikomanagement gibt zwar den Anstoss für den Aufbau von Vorkehrungen zum Notfall-, Krisen- und Kontinuitätsmanagement, befasst sich aber nicht selber mit den Vorbereitungen und mit der Krisenbewältigung.

Das Krisenmanagement ist eine Ergänzung des Risikomanagements, weil es sich ausschliesslich auf die Phase nach Eintritt eines gravierenden Risikos konzentriert. Die Früherkennung von Notfällen und Krisen ist eine Schnittstelle zwischen Risiko- und Krisenmanagement. Das Wissen über die mögliche Entwicklung von Risiken erlaubt eine Früherkennung von sich anbahnenden Krisen. Die Früherkennung von Krisen erfolgt daher implizit anlässlich der Überwachung der Risiken und ist ein integraler Bestandteil des Risikomanagements. Im Rahmen des Risikomanagements muss sichergestellt werden, dass frühzeitig Vorbereitungsmassnahmen gegen sich anbahnende Notfälle und Krisen ergriffen werden (Aufbau Krisenorganisation, Übungsszenarien usw.) und dass das Notfall- und Krisenmanagement gegebenenfalls rechtzeitig aktiviert werden können. Für die Früherkennung von möglichen Krisen kann es hilfreich sein, die «Innenansicht» der Organisation mit einer «Aussensicht» zu ergänzen, bei der Entwicklungen beobachtet werden, die noch nicht unmittelbar Auswirkungen auf die Organisation haben, bzw. die von externen Experten anders eingeschätzt werden als von internen. Die Erkenntnisse, welche auf diese Weise erlangt werden, müssen in die Risikobeurteilung zurückfliessen.

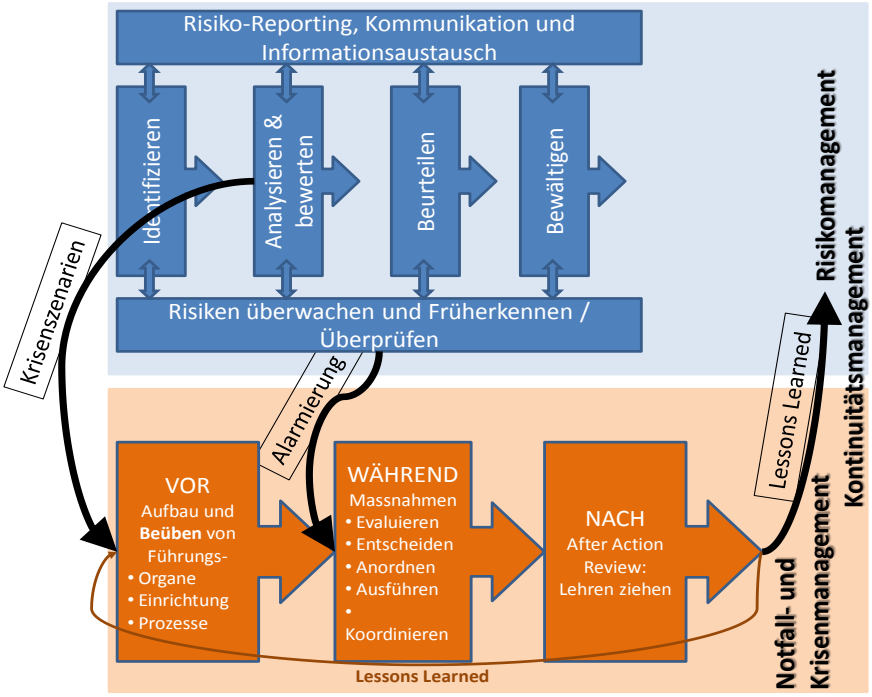


Abbildung 16: Schnittstelle Risikomanagement und Krisenmanagement

In der Bundesverwaltung haben sich mehrere Organisationseinheiten und Strukturen entwickelt und etabliert, die direkt oder indirekt mit Notfall- und Krisenmanagement zu tun haben. Es sind einerseits Organe für die Bewältigung von besonderen und ausserordentlichen Lagen (Krisenstäbe der Departemente und der BK sowie interdepartementale Sonderstäbe) und andererseits Organisationen mit dem Schwergewicht auf der Früherkennung. Während Erstere punktuell beim Eintritt einer Krise aktiv werden, ist die Früherkennung ein ständig laufender Prozess. Die nachfolgende Abbildung soll einen Überblick verschaffen.

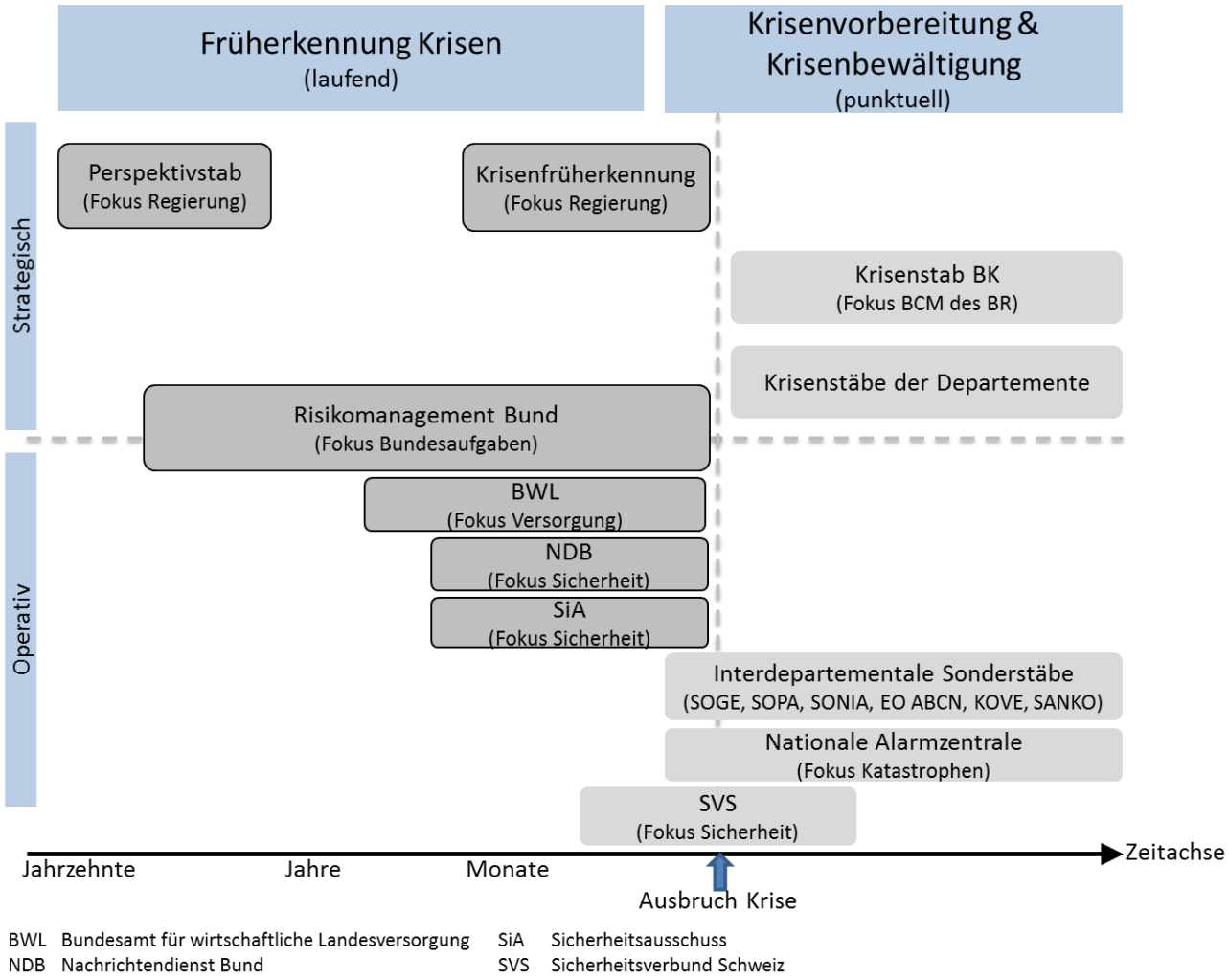


Abbildung 17: Überblick Krisenmanagement-Organisationen

Die diversen Organe im Bereich der Krisenfrüherkennung haben einen unterschiedlichen Fokus und einen unterschiedlichen Zeithorizont. Sie ergänzen sich und ermöglichen den übergeordneten Hierarchiestufen einen breiteren Überblick. Die in der BK angesiedelte Krisenfrüherkennung[49] operiert auf einer kurzfristigen (bis max. 1,5 Jahre) strategischen Ebene. Sie ergänzt die bisherigen Instrumente durch eine zusätzliche Aussensicht der aktuellen Situation. Damit sollen bei Ereignissen, bei denen es mehr als eine Meinung bezüglich Krisenpotenzial und eventueller Auswirkungen gibt, alternative Einschätzungen (zweite Meinungen) sichtbarer werden.

Schnittstellen zum Risikomanagement:
Das Notfall- und Krisenmanagement ist Teil des Risikomanagements. Das Risikomanagement stellt sicher, dass rechtzeitig die notwendigen Massnahmen für den Aufbau und die zeitgerechte Aktivierung eines effizienten Notfall- und Krisenmanagements getroffen werden.

Notwendiger Informationsaustausch:
1. Mindestens halbjährlicher Abgleich mit den anderen Organen der Krisenfrüherkennung.

[49] Gesetzlicher Auftrag gemäss Art. 32 Bst. g und Art. 33 Abs. 1bis RVOG (in Kraft seit 1. Januar 2015).

2. Bei Risiken mit potenziell grossen Auswirkungen wird die Linie auf ihre Verantwortung bezüglich Vorbereitung eines Notfall- und Krisenmanagements hingewiesen. Diese Risiken sind als Übungsszenarien des Notfall- und Krisenmanagements zu übernehmen.
3. Die Früherkennung von Krisen dient der zeitgerechten Alarmierung des Notfall- und Krisenmanagements.
4. Die relevanten Lehren aus der Bewältigung von Notfällen und Krisen werden im Risikomanagement berücksichtigt.

6.3 Kontinuitätsmanagement

Im Kontinuitätsmanagement (englisch: Business Continuity Management, BCM) werden alle notwendigen Vorkehrungen getroffen, so dass die Bundesverwaltung und der Bundesrat ihre Kernaufgaben selbst in ausserordentlichen Situationen termingerecht erfüllen können. In einem ersten Schritt müssen die relevanten kritischen Geschäftsprozesse ermittelt werden, die zur Erfüllung der Kernaufgaben notwendig sind. Ausgehend von dieser Basis kann danach beurteilt werden, welche Risikoszenarien möglich sind und welche Auswirkungen diese auf die kritischen Prozesse haben können (*Business Impact Analysis*). Grundsätzliche Vorgehensweisen im Krisen/Katastrophenfall werden in einer *Business Continuity Strategy* festgehalten und kommuniziert. Im *Business Continuity Planning* werden sodann konkrete Pläne zur Wiederherstellung bzw. Fortsetzung von geschäftskritischen Prozessen erstellt, beispielsweise Vorgehensweisen und Ersatzressourcen (Notebooks, Arbeitsplätze). Da die Sicherstellung der Kontinuität von Geschäftsprozessen i.d.R. mit hohen Kosten verbunden ist (z.B. Redundanzen), müssen auch im Kontinuitätsmanagement die Kosten einer Massnahme gegen den Nutzen abgewogen werden.

Die Verantwortung für das BCM soll nach einem Entscheid der GSK aus dem Jahre 2009 grundsätzlich bei den einzelnen Departementen bleiben. Der Bundesrat hat 2010 beschlossen[50], dass die Bundeskanzlei in Zusammenarbeit mit den Departementen eine minimale Richtlinie für die Business-Continuity-Planung (BCP) «Strommangellage» erlässt. Die Departemente ihrerseits haben sicherzustellen, dass ihre BCP den Fall einer Strommangellage abdecken. Am 19. Dezember 2011 wurde die von der BK in Zusammenarbeit mit den Departementen erstellte minimale Richtlinie (am Szenario Strommangellage) durch die GSK verabschiedet und den Departementen zur Umsetzung übergeben. Die Richtlinie kann szenariounabhängig von den Departementen zur Etablierung eines BCM verwendet werden.

Ein zweckmässiges Kontinuitätsmanagement ist Teil des Risikomanagements. Mit dem Aufbau eines Kontinuitätsmanagements können die Auswirkungen eines Risikos, das trotz vorbeugender Massnahmen eintreten kann und wichtige Geschäftsprozesse der BV stark beeinträchtigt, minimiert werden. Es ist aus Sicht Risikomanagement als Massnahme gegen Risiken mit Auswirkung auf die Geschäftsprozesse zu betrachten.

Sinnvollerweise wird bei der Risikoanalyse im Rahmen des regelmässigen Risikomanagement-Prozesses untersucht, ob und welche Risiken wichtige Geschäftsprozesse beeinträchtigen und in welchen Fällen der Aufbau eines Kontinuitätsmanagements als Bewältigungsmassnahme notwendig und sinnvoll ist.

Schnittstellen zum Risikomanagement:
Organisatorisch existiert keine Schnittstelle, da bundesweit keine für Kontinuitätsmanagement zuständigen Organisationen aufgebaut wurden. Auf inhaltlicher Ebene werden vor-

[50] vgl. Bundesratsbeschluss 18.06.2010

handene Kontinuitätsmanagement-Konzepte bei den entsprechenden Risiken im Risikomanagement Bund kurz als Massnahmen erläutert, die eine mindernde Auswirkung auf die Höhe des Risikos haben.

Notwendiger Informationsaustausch:
Ein allgemeiner Erfahrungsaustausch zum Thema Kontinuitätsmanagement und in einzelnen Bereichen umgesetzte Konzepte findet innerhalb der departementsübergreifenden Risikomanager-Workshops statt.

6.4 Perspektivstab

Kernauftrag des Perspektivstabs ist die Erarbeitung einer Lage- und Umfeldanalyse als Grundlage für die Legislaturplanung mit der Darstellung der sich daraus ergebenden wichtigsten Herausforderungen, die in den kommenden 10 bis 15 Jahren auf die Schweiz im Allgemeinen und auf die Bundespolitik im Besonderen zukommen können. Diese leiten sich aus einer Trendanalyse sowie aus den für vier verschiedene Szenarien relevanten Chancen, Gefahren und Hauptherausforderungen ab. Berücksichtigt werden sowohl externe als auch interne Entwicklungen, indem verwaltungsinterne und externe Expertinnen und Experten aus Wissenschaft, Wirtschaft und Gesellschaft im Rahmen von Workshops und Fokusgesprächen am Prozess mitwirken. Der Zweck des Produktes «Perspektiven 2030» ist es, einen Beitrag zu einer vorausschauenden und kohärenten Regierungspolitik zu leisten.

Im Vergleich zum Risikomanagement fokussiert der Perspektivstab v. a. auf Themen, die strategisch politischer Natur sind und einen direkten Bezug zur Regierungstätigkeit haben. Auch konzentriert er sich auf Herausforderungen im mittel- bis langfristigen Zeithorizont (vgl. Abbildung 17). Aus den durch den Perspektivstab erkannten mittel- bis langfristigen Herausforderungen können im Verlaufe der Zeit konkrete Risiken mit Bezug zu Bundesaufgaben und auch Krisen entstehen. Deshalb ist ein Informationsaustausch zwischen dem Perspektivstab und dem Risikomanagement Bund unabdingbar.

Schnittstellen zum Risikomanagement:
Die im Perspektivstab identifizierten Herausforderungen stellen zum Zeitpunkt der Identifikation noch abstrakte Gefahren dar. Im Verlauf der Zeit können daraus konkrete Risiken entstehen, die im Risikoreporting der Bundesverwaltung aufgenommen werden müssen.

Notwendiger Informationsaustausch:
Der Informationsaustausch ist dadurch sichergestellt, dass mindestens ein Vertreter der Koordinationsstelle Risikomanagement punktuell in die Erarbeitung der neuen Lage- und Umfeldanalyse eingebunden ist.

6.5 Corporate Governance[51]

Bundesaufgaben werden teilweise durch im Eigentum des Bundes stehende, rechtlich, organisatorisch und finanziell verselbständigte Einheiten wahrgenommen. Damit der Bundesrat

[51] Zur Corporate Governance des Bundes: Vgl. Bericht des Bundesrates vom 13. September 2006 zur Auslagerung und Steuerung von Bundesaufgaben (Corporate-Governance-Bericht, BBl **2006** 8233); Zusatzbericht des Bundesrates vom 25. März 2009 zum Corporate-Governance-Bericht – Umsetzung der Beratungsergebnisse des Nationalrats (Zusatzbericht, BBl **2009** 2659); Erläuternder Bericht der Eidgenössischen Finanzverwaltung vom 13. September 2006 zum Corporate-Governance-Bericht des Bundesrates (Erläuternder CG-Bericht EFV).

seine Eigner- und Gewährleistungsfunktion[52] gegenüber diesen Einheiten wahrnehmen kann, macht er ihnen im Rahmen der Corporate Governance des Bundes[53] Vorgaben (strategische Ziele). Hierzu zählt auch die Führung eines Risikomanagements, wozu die obersten Leitungsorgane der Organisationen durch die Gesetzgebung oder entsprechende strategische Vorgaben des Bundes verpflichtet sind. Die für die Steuerung der verselbständigte Einheiten zuständigen Fachdepartemente sind gemäss dem Bundesratsbeschluss vom 19. Januar 2005 zur Risikopolitik des Bundes gehalten, anlässlich der periodischen Beurteilung der Einhaltung der Eignerstrategie darauf zu achten, dass die ihnen zugeordneten verselbständigten Einheiten ein angemessenes Risikomanagement umsetzen (Kontrolle der Existenz und der Angaben über die Durchführung im Geschäftsbericht). Übernimmt der Bund gegenüber einzelnen verselbständigten Einheiten spezifische Haftungen, Garantien, Bürgschaften und Eventualverpflichtungen, müssen eingehendere, risikopolitische Vorgaben (z.B. Vorgaben zur Vermeidung oder Verminderung bestehender Risiken, Versicherungspflicht, Reservenbildung) gemacht und deren Einhaltung regelmässig und umfassender überprüft werden[54].
Das Risikomanagement des Bundes steht den ausgelagerten Einheiten als Sparring-Partner oder Coach zu methodischen Fragen und Themen rund ums Risikomanagement zur Verfügung. Durch einen gegenseitigen Erfahrungsaustausch kann das Risikomanagement sowohl bei den ausgelagerten Einheiten wie auch in der Bundesverwaltung verbessert werden.

Schnittstellen zum Risikomanagement:
Organisatorisch bestehen keine Schnittstellen zwischen dem Risikomanagement des Bundes und dem Risikomanagement der Einheiten; die Zuständigkeiten sind klar getrennt. Inhaltlich können aber Überschneidungen bestehen:

- Bestehen spezifische Haftungen, Garantien und Bürgschaften des Bundes (z.B. in Bezug auf die Ausfallhaftung gemäss Art. 19 VG) für die verselbständigten Einheiten, so sind sie zwingend Gegenstand des Risikomanagements des Bundes.
- Auch wenn keine spezifischen Haftungen, Garantien und Bürgschaften des Bundes bestehen, kann sich dieser im Einzelfall veranlasst sehen, bei einer Veränderung der Risikosituation bei verselbständigten Einheiten, deren Risikofähigkeit zu stärken (z.B. Rekapitalisierung usw.).
- Durch die Eigner- und Gewährleistungsfunktion des Bundesrates und die damit verbundenen Steuerungs- und Kontrollaufgaben bleibt die Verantwortung für die Erfüllung dieser Aufgaben beim Bundesrat, der auch nach einer Auslagerung die politische Gesamtverantwortung und die damit verbundenen Risiken trägt[55].

Notwendiger Informationsaustausch:
Ein Austausch ist sinnvoll bezüglich

- methodischen Themen rund um das Risikomanagement;
- Risiken des Bundes, die sich direkt aus der Eigner- und Gewährleistungsfunktion sowie der politischen Gesamtverantwortung des Bundesrates ergeben.

[52] Zusatzbericht, Ziff. 6.2, Leitsatz 16.

[53] Zum Begriff: Erläuternder CG-Bericht EFV, Ziff. II/2.

[54] Corporate-Governance-Bericht, Ziff. 4.2.4 a. E., Leitsatz 12; Erläuternder CG-Bericht EFV, Ziff. I/5.4. Diese umfassendere Überprüfung kann allenfalls im Rahmen eines entsprechenden Auftrages durch die Revisionsstelle erfolgen.

[55] Art. 8 Abs. 4 RVOG

6.6 Versicherungsmanagement

Die Grundlagen des Versicherungsmanagements des Bundes sind in der Finanzhaushaltsverordnung geregelt.[56] Der Bund trägt als Eigenversicherer das Risiko für Schäden an seinen Vermögenswerten und für die haftpflichtrechtlichen Folgen seiner Tätigkeit grundsätzlich selbst. Ausnahmsweise kann ein Risiko durch den Abschluss eines Versicherungs- oder Schadenerledigungsvertrag durch einen Dritten bewirtschaftet werden, insb. wenn das Risiko ein hohes Schadenpotential aufweist, das Fachwissen für die Schadenerledigung fehlt oder wenn die Risikoüberwälzung wirtschaftlich ist.[57] Bei Abschluss von Versicherungen ist zu beachten, dass die Vertragskonditionen ein optimales Preis-Leistungs-Verhältnis aufweisen und den Marktverhältnissen entsprechen. In der Bundesverwaltung wird die Bewirtschaftung von Versicherungen zentral durch die Koordinationsstelle EFV geführt. Dadurch ergeben sich *organisatorisch* keine Schnittstellen mit dem Risikomanagement. Im Gegenteil können Analysen und Bewertungen aus dem Risikomanagement genutzt werden, um allfällige Versicherungslösungen zu beurteilen.

Schnittstellen zum Risikomanagement:
Da die Koordinationsstelle EFV gleichzeitig auch das zentral geführte Versicherungsmanagement führt, ergeben sich in diesem Bereich keine organisatorischen Schnittstellen und es muss kein Informationsaustausch festgelegt werden.

6.7 Informatiksteuerungsorgan des Bundes

Das Informatiksteuerungsorgan des Bundes (ISB) steuert und führt den Einsatz der IKT des Bundes. Zwischen den Aufgaben des ISB und dem Risikomanagement des Bundes bestehen insbesondere folgende zwei Schnittstellen:

IKT-Sicherheit
Die Anforderungen an die IKT-Sicherheit, um für die IKT-Schutzobjekte der Bundesverwaltung einen angemessenen Schutz der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit zu gewährleisten, sind in den Weisungen des Bundesrats vom 1. Juli 2015 über die IKT-Sicherheit in der Bundesverwaltung[58] und in den darauf basierenden Vorgaben des ISB zum Sicherheitsverfahren festgelegt. Die Sicherheitsmassnahmen orientieren sich an den jeweils aktuellen ISO-Standards betreffend die IKT-Sicherheitsverfahren. Die operative Umsetzung der IKT-Sicherheitsanforderungen liegt bei den einzelnen VE. Die Risiken aus IKT-Projekten und aus dem IKT-Betrieb werden identifiziert, bewertet und durch angemessene Massnahmen im Rahmen des Sicherheitsverfahrens reduziert bzw. eliminiert. Restrisiken müssen der Leitung der VE bekannt sein und von ihr bewusst in Kauf genommen werden. Basierend auf einer strukturierten Umfrage bei den Informatiksicherheitsbeauftragten der Stufe Departement, den eigenen Erfahrungen und Feststellungen sowie den eingegangenen Sicherheitsmeldungen verfasst das ISB zuhanden des Bundesrates jährlich einen Informatiksicherheitsbericht Bund. Es muss sichergestellt werden, dass in diesem Bericht aufgeführte wesentliche Risiken im Rahmen des Risikomanagements analysiert werden.

Schnittstelle Strategisches IKT-Controlling
Seit April 2013 legt der Bundesrat die IKT-Schlüsselprojekte des Bundes fest. IKT-Schlüsselprojekte sind IKT-Projekte oder IKT-Programme, die aufgrund ihres Ressourcenbedarfs, ihrer strategischen Bedeutung, ihrer Komplexität, ihrer Auswirkungen oder ihrer Risiken eine verstärkte übergeordnete Führung, Steuerung, Koordination und Kontrolle erfordern. Die Aufgaben und Verantwortlichkeiten im Zusammenhang mit den IKT-Schlüsselprojekten sind in

[56] Art. 50 FHV
[57] Vgl. Weisungen über die Risikotragung und Schadenerledigung beim Bund, Ziff. 1.2.
[58] Vgl. BBl *2015* 5795

den Weisungen des Bundesrates vom 1. Juli 2015 zu den IKT-Projekten in der Bundesverwaltung und zum IKT-Portfolio des Bundes[59] geregelt. Die Verantwortlichen der IKT-Schlüsselprojekte erstatten zuhanden des ISB halbjährlich einen Statusbericht, welcher die für die Oberaufsicht relevanten Informationen umfasst. Das ISB konsolidiert diese Berichte zu einem einzigen Gesamtbericht und erstellt im Rahmen des Strategischen IKT-Controllings zuhanden des Bundesrates eine Zusammenfassung der wichtigsten von der EFK im Rahmen ihrer Prüfungen der IKT-Schlüsselprojekte erstellten Prüfergebnisse. Das ISB unterbreitet den Bericht zum Stand der IKT-Schlüsselprojekte des Bundes dem Bundesrat, welcher auf diese Weise die Finanzdelegation der eidgenössischen Räte halbjährlich informiert. Nach Ziffer 4.4 der erwähnten Weisungen ist es Aufgabe der zuständigen VE, die Risiken ihrer IKT-Schlüsselprojekte nach den Vorgaben des Risikomanagements Bund zu identifizieren, zu analysieren und zu bewerten. Sie melden und überwachen jene Risiken, die wesentliche negative Auswirkungen auf die Erreichung der Ziele und die Erfüllung der Aufgaben der Bundesverwaltung haben können. Damit sichergestellt ist, dass schwerwiegenden Problemen bei IKT-Schlüsselprojekten auch aus Sicht des Risikomanagements Bund nachgegangen wird, meldet die Koordinationsstelle EFV den Risikomanagern der betroffenen Departemente raschmöglichst alle «roten» Projekte auf dem Controlling-Bericht des ISB. Der Risikomanager klärt ab, ob das rote Schlüsselprojekt als Risiko erfasst, korrekt analysiert und wie es zu bewerten ist. Er informiert anschliessend die Koordinationsstelle über den Stand aus Sicht Risikomanagement Bund.

Schnittstellen zum Risikomanagement:
Probleme bei der IKT-Sicherheit generell oder im Zusammenhang mit IKT-Projekten können die Aufgabenerfüllung oder Zielerreichung der Bundesverwaltung gefährden. Die periodischen Berichte des ISB zu diesen Themen können für das Risikomanagement Bund wertvolle Informationen enthalten. Umgekehrt ist es auch möglich, dass aufgrund der Risikoberichterstattung Lücken in den Berichten des ISB festgestellt werden.

Notwendiger Informationsaustausch:
Periodischer Abgleich zwischen dem Risikomanagement Bund und der ISB-Berichterstattung (IKT-Sicherheitsbericht, Strategischer IKT-Controllingbericht), gegenseitige Orientierung bei besonderen Vorkommnissen, Sicherstellung des Wissensaustausches.

6.8 Eidgenössische Finanzkontrolle (EFK)

Die Eidgenössische Finanzkontrolle (EFK) ist das oberste Finanzaufsichtsorgan des Bundes. Sie unterstützt das Parlament und den Bundesrat, ist unabhängig und nur Verfassung und Gesetz verpflichtet. Der Aufgabenbereich ist im Finanzkontrollgesetz geregelt. Die EFK prüft das Finanzgebaren der Bundesverwaltung und zahlreicher halbstaatlicher und internationaler Organisationen. Massgebend bei ihren Prüfungen sind die Kriterien der Wirtschaftlichkeit und Wirksamkeit, der Ordnungs- und Rechtmässigkeit.

In ihrem Bericht zum Informatikprojekt «INSIEME» haben die Finanz- und Geschäftsprüfungskommissionen dem Bundesrat empfohlen, dass die jährliche Berichterstattung der EFK über wichtige Umsetzungspendenzen («Revisionspendenzen») – d. h. alle offenen Empfehlungen der höchsten Wichtigkeitsstufe – angemessen in das Risikomanagement des Bundes sowie in das jährliche Risikoreporting des Bundesrates an die GPK einfliessen sollen. Der BR wies in seiner Stellungnahme[60] daraufhin, dass Umsetzungspendenzen Hinweise über eine ungenügende Aufgabenerfüllung oder Zielerrichung der Bundesverwaltung beinhalten

[59] Vgl. BBl *2015* 5801
[60] Vgl. BBl *2015* 6745

können. Er hat die Empfehlung deshalb angenommen. Sie wird ab 2015 umgesetzt. Jede VE bzw. jedes Departement ist im Rahmen des Risikomanagementprozesses dafür verantwortlich, dass die (wichtigsten) Revisionspendenzen im Risikomanagement berücksichtigt werden (normaler Prozess). Als zusätzliches Controllinginstrument werden die Umsetzungspendenzen einmal jährlich zwischen der EFK und der Koordinationsstelle Risikomanagement Bund besprochen. Resultate aus diesem Validierungsgespräch fliessen anschliessend mittels Rückfragen der EFV zurück an die entsprechenden VE resp. das entsprechende Departemente. Dadurch ist sichergestellt, dass der Austausch sowohl über den ordentlichen Prozess, als auch durch Rückfragen der Koordinationsstelle Risikomanagement Bund optimiert wird.

Schnittstellen zum Risikomanagement:
Revisionspendenzen der EFK können Hinweise auf eine ungenügende Aufgabenerfüllung oder Zielerreichung der VE und Departemente enthalten und sind daher im Rahmen des Risikomanagementprozesses zu berücksichtigen.

Notwendiger Informationsaustausch:
Abgleich mit dem jährlichen Bericht der EFK über die wichtigsten Umsetzungspendenzen («Revisionspendenzen Prio. A»).

6.9 Weitere Schnittstellen

In der Bundesverwaltung existieren auch Projekte, die sich mit besonderen Themen des Risikomanagements beschäftigen. Der Informationsaustausch und die Abgrenzung werden im Anhang 8 erläutert. Dieser Anhang wird regelmässig aktualisiert.

7 Verbesserung des Risikomanagements Bund

Das Risikomanagement in der Bundesverwaltung wird stetig weiterentwickelt und verbessert.[61] Die Risikocoaches, die Risikomanager und die Koordinationsstelle EFV nutzen Erkenntnisse aus ihrer Risikomanagementtätigkeit in der Bundesverwaltung um Verbesserungen des Risikomanagements vorzuschlagen und allenfalls umzusetzen. Auf Stufe Bundesrat ist die Koordinationsstelle EFV zuständig für den Entscheid und die Umsetzung von Verbesserungsmassnahmen des Risikomanagements. Auch bundesverwaltungsexterne Inputs (z.B. Risikomanagementveranstaltungen) tragen dazu bei, Verbesserungspotential des bundesweiten Risikomanagements zu erkennen. Die Richtlinien und das vorliegende Handbuch werden nach Bedarf regelmässig angepasst.

7.1 Leistungsbewertung

Um das Risikomanagement in der Bundesverwaltung laufend zu verbessern, muss dessen Leistung regelmässig bewertet werden. Es können dabei zwei Dimensionen unterschieden werden: die inhaltliche Verbesserung, d.h. die Veränderung des Risikoprofils (der Gesamtheit der Risiken) der Bundesverwaltung und die organisatorische Verbesserung, d.h. inwiefern ein effektives Risikomanagementsystem aufgebaut wurde und umgesetzt wird.

Bei der *inhaltlichen* Verbesserung können entweder auf risikoindividueller oder aggregierter Stufe Aussagen erarbeitet werden, wie stark das Risiko bzw. das aggregierte Risikopotential der Bundesverwaltung vermindert werden konnte. Da in der Bundesverwaltung auf eine quantitative Aggregation verzichtet wird, konzentriert sich das Risikomanagement Bund auf die grössten Einzelrisiken und inwiefern diese reduziert werden konnten. Die Veränderungen der Risiken werden in den Berichterstattungen auf Stufe Bund, Departement / BK und VE dargestellt.

Bei der *organisatorischen* Verbesserung geht es um die Prüfung, wie weit der Aufbau eines effektiven Risikomanagement-Systems erfolgt ist und ob dieses in der Praxis umgesetzt wird. Diese Prüfung erfolgt meistens mit Hilfe eines Audits/Reviews.
Zusätzlich sollte regelmässig untersucht werden, ob in einer Organisation allgemeine Strukturen und Eigenheiten vorliegen, welche die Effektivität des Risikomanagementprozesses beeinträchtigen und eine allmähliche Entwicklung von Risiken begünstigen können (vgl. Anhang 9).

7.2 Audit / Review

Mittelfristig soll in der Bundesverwaltung das Risikomanagement durch ein internes oder externes Audit regelmässig geprüft werden. Diese Audits werden sich voraussichtlich auf folgende Fragen im Zusammenhang mit dem Risikomanagement-System konzentrieren:

- Existiert ein Commitment der obersten Leitung, das Risikomanagement umzusetzen?
- Umfasst das Risikomanagement alle Bereiche der Bundesverwaltung?
- Existiert eine von der Leitung genehmigte Risikopolitik?
- Sind die Risikoeigner, Risikomanager und Risikocoaches benannt und nehmen sie ihre Aufgaben wahr?
- Existiert eine angemessene interne und externe Risikokommunikation?
- Verfügen Risikomanager und Risikocoaches über die passende Eignung, Ausbildung

[61] Ziff. 4 Abs. 8 der Weisungen

und Erfahrung?

- Ist das Risikomanagement in wichtigen Prozessen der Bundesverwaltung integriert?
- Passen die verwendeten Methoden zu den Anwendungsgebieten?
- Sind die Risikobeurteilungen dokumentiert und von den Risikoeignern freigegeben worden?
- Sind Massnahmen zur Risikobewältigung umgesetzt und werden dies auf ihre Wirksamkeit überprüft?
- Wird die Wirksamkeit des Risikomanagements (inkl. die Aufgabenerfüllung durch die Koordinationsstelle EFV) regelmässig von einer unabhängigen Stelle bewertet?
- Ist das Risikomanagement-System gut dokumentiert, sind die Dokumente auffindbar und aktuell?

7.3 Zertifizierung

Bei ISO 31000:2009 handelt es sich um eine Richtlinie («Guideline») und nicht um einen zertifizierbaren Standard. Die Koordinationsstelle EFV wird die weitere Entwicklung in diesem Bereich verfolgen.

Anhang 1: Begriffsdefinitionen

In diesem Anhang werden in alphabetischer Reihenfolge Begriffe definiert und erläutert, die im Risikomanagement Bund verwendet werden. Für die Funktionen und Verantwortlichkeiten im Risikomanagement Bund wird auf Ziffer 2.2 verwiesen. Die Begriffe werden im Rahmen von Risikomanagement Bund einheitlich verwendet. Dadurch wird die Kommunikation verbessert und ein gemeinsames Verständnis geschaffen. Die nachfolgenden Definitionen lehnen sich im Allgemeinen an gängige Normen an. Diese enthalten weitere Begriffsdefinitionen, auf die hier verwiesen werden kann.

Akzeptiertes Risiko: Risiko, das z. B. aus technischen, praktischen oder wirtschaftlichen Gründen nicht (weiter) reduziert werden soll und somit getragen wird.

Auswirkung: Folge eines Ereignisses oder einer Entwicklung, die zu einer Beeinträchtigung der Ziele oder der Aufgabenerfüllung der Bundesverwaltung führt (Abweichung von ONR Norm 49000). Die verschiedenen Auswirkungsdimensionen werden in Ziffer 3.3.4 näher erläutert.

Bedrohung: Potenzielle Quelle eines Risikos, die zu einer ungünstigen Entwicklung führen kann.

Bereichsrisiken: Alle auf Stufe Verwaltungseinheit identifizierten und bewirtschafteten Risiken.

Bottom-up-Ansatz: Vorgehensweise bei der Risikobeurteilung, bei der die Einzelteile der Organisation auf der untersten Stufe Gegenstand der Risikoidentifikation und der Risikoanalyse sind. Die Risiken werden entlang der Linienorganisation nach oben gemeldet und dort konsolidiert.

Brainstorming: Methode, bei der im Rahmen einer Gruppe eine Vielfalt von Ideen gesammelt, bewertet und geordnet werden. Das Sammeln der Ideen erfolgt ohne Einschränkungen, jegliche Kritik ist verboten. Bei der Bewertung und Ordnung geht es darum, problemferne Ideen auszusortieren und thematisch verwandte Ideen zu gruppieren.

Bundesratsrisiken: Die für den Bundesrat wichtigsten Risiken, die in einem Konsolidierungsprozess aus allen Risiken der Bundesverwaltung und nach Überprüfung durch die GSK an den Bundesrat gemeldet werden.

Bundesverwaltung: Sie untersteht dem Bundesrat und umfasst die Departemente und die Bundeskanzlei. Die einzelnen Departemente gliedern sich in Ämter, die zu Gruppen zusammengefasst werden können und sie verfügen je über ein Generalsekretariat. Zur Bundesverwaltung gehören ferner dezentralisierte VE nach Massgabe ihrer Organisationserlasse.[62]

Departementsrisiken: Alle von den VE an das Departement gemeldeten Risiken. Dies sind die grössten Risiken je VE und alle Risiken, die eine definierte Risikohöhe überschreiten.

Entwicklung: Eine allmähliche Veränderung von Umständen.

Ereignis: Plötzlicher Eintritt einer bestimmten Kombination von Umständen.

[62] Art. 2 RVOG

Gefahr: Potenzielle Quelle eines Risikos, die zu einem plötzlich eintretenden Schadenereignis führen kann.

Internes Kontrollsystem: Das IKS umfasst alle regulatorischen, organisatorischen und technischen Massnahmen, die eingeführt werden, um identifizierte Risiken in der Organisation zu minimieren. Das IKS in der Bundesverwaltung konzentriert sich insbesondere auf die finanzrelevanten Geschäftsprozesse.

Kernrisiken: Alle von den Departementen und der Bundeskanzlei an die Koordinationsstelle EFV gemeldeten Risiken Dies sind die grössten Risiken je Departement / der BK und alle Risiken, die eine definierte Risikohöhe überschreiten.

Kontinuitätsmanagement (Business Continuity Management, BCM): Im Kontinuitätsmanagement werden alle notwendigen Vorkehrungen getroffen, damit die Bundesverwaltung und der Bundesrat ihre Kernaufgaben selbst in ausserordentlichen Situationen termingerecht erfüllen können (Abweichung von ONR Norm 49000).

Krise: Situation, die organisationsweit ausserordentliche Massnahmen erfordert. Im Gegensatz zu einem Notfall bezieht sich eine Krise auf eine Organisation: eine Organisation (oder System/Institution) befindet sich in einer Krise, wenn ihre Reputation (Glaubwürdigkeit, Vertrauen), ihr Handlungsspielraum oder ihre Existenz gefährdet ist.

Krisenfrüherkennung: Auseinandersetzung mit Ereignissen und Trends, die bereits sichtbar sind und ein Potenzial besitzen, sich meist in einer Zeitspanne von Monaten bis max. 1,5 Jahren zu Krisen zu entwickeln.

Massnahmenverantwortlicher: Person, die für die konkrete Umsetzung einer Massnahme zur Reduktion eines Risikos verantwortlich ist und vom Risikoeigner einen entsprechenden Auftrag erhält.

Nettorisiko: Der Teil eines Risikos, der nach Umsetzung von Risikobewältigungsmassnahmen verbleibt.

Notfall: Plötzliches und für gewöhnlich unvorhergesehenes Ereignis mit schwerwiegenden negativen Folgen, das ein rasches Eingreifen erfordert. Im Gegensatz zu einer Krise bezieht sich ein Notfall auf ein Ereignis, das einen Schadenplatz anrichtet (geografisch abgrenzbar), der so schnell als möglich aufzuräumen respektive zu beheben ist.

Organisationseinheit: Gruppe von Personen und Einrichtungen mit einem Gefüge von Verantwortungen, Befugnissen und Beziehungen. Der Begriff OE kann sich auf die Bundesverwaltung als Ganzes, ein Departement / die BK, eine VE oder kleinere Einheiten beziehen.

Quellrisiko: Einzelrisiko, das mit anderen Risiken auf übergeordneter Ebene zu einem Querschnittsrisiko aggregiert wird.

Querschnittsrisiken*:* Ereignisse oder Entwicklungen, die sich beim Eintritt in mehreren VE gleichzeitig negativ auswirken oder unabhängig voneinander in mehreren VE gleiche oder ähnliche negative Auswirkungen auf die Aufgabenerfüllung und Zielerreichung haben können. *Beispiele:* Grossflächiger IKT-Ausfall, Pandemie, Erdbeben, Korruption etc.

Restrisiko[63]***:*** Im Risikomanagement Bund werden in den drei gängigen Anwendungsfällen präzisere Begriffe verwendet (Abweichung von ONR 49000): -> Akzeptiertes Risiko -> Nettorisiko -> Unerkanntes Risiko

Riskmap: Darstellung, in der Risiken entsprechend ihren Auswirkungen und der Eintrittswahrscheinlichkeit graphisch eingeordnet werden.

Risiko: Ereignisse und Entwicklungen, die mit einer gewissen Wahrscheinlichkeit eintreten und wesentliche negative finanzielle und nichtfinanzielle Auswirkungen auf die Erreichung der Ziele und die Erfüllung der Aufgaben der Bundesverwaltung haben (Abweichung von ONR Norm 49000).[64]

Risikoaggregation*:* Verfahren, das mehrere Risiken auf übergeordneter Ebene zusammenfasst. Die Berichterstattung und zum Teil die Bewirtschaftung des aggregierten Risikos (übergreifende Massnahmen) erfolgen dann auch auf übergeordneter Ebene. *Beispiel:* Ein IKT-Ausfall in der EFV und einer in der ESTV können aggregiert werden, wenn bei beiden Risiken die Ursache dieselbe ist, z. B. ein Stromunterbruch im Gebäude, in welchem beide Systeme betrieben werden.

Risikoaggregation (quantitativ)[65]***:*** Verfahren, welches das Zusammenwirken mehrerer, voneinander eventuell abhängiger Einzelrisiken zu einem Gesamtrisiko (VaR) ermittelt und aufzeigt.

Risikoakzeptanz: Entscheidung, ein Risiko zu tragen.

Risikoakzeptanzschwelle: Pro OE definierte Risikohöhe, ab der Bewältigungsmassnahmen ins Auge gefasst werden sollen.

Risikoart: Unterteilung von Risiken nach unterschiedlichen Kriterien.

Risikobeurteilung: Prozess, der die Ergebnisse der Risikobewertung mit der Risikotoleranz vergleicht, um zu bestimmen, ob die Risikohöhe akzeptierbar bzw. tolerierbar ist (Abweichung von ONR Norm 49000).

Risikobewältigung: Auswahl und Umsetzung von Massnahmen, um ein Risiko zu vermeiden oder zu vermindern. Das Notfall-, Krisen- und Kontinuitätsmanagement sind auch Bestandteile der Risikobewältigung.

Risikobewertung: Systematische Ermittlung und Gebrauch von Informationen, um ein Risiko zu verstehen und nach Eintrittswahrscheinlichkeit und Auswirkungen auf die Bundesverwaltung einzuschätzen (Abweichung von ONR Norm 49000).

Risikocoach: Person, die den Risikomanagement-Prozess auf Stufe VE anwendet und umsetzt und für die Einbettung des Risikomanagements in der VE zuständig ist.

Risikoeigner: Person mit der Entscheidungskompetenz und Verantwortung, hinsichtlich eines Risikos zu handeln. Der Risikoeigner kann hierarchisch auf allen Stufen innerhalb der Bundesverwaltung angesiedelt sein (Mitarbeiter mit Entscheidungskompetenz bezüglich dem konkreten Prozess, Bundesrat als kollektiv handelndes Entscheidungsorgan).

---

[63] Vgl. Brühwiler, B. (2007). *Risikomanagement als Führungsaufgabe*. (2. Auflage). Bern: Haupt Verlag.

[64] Ziff. 2 Abs. 1 der Weisungen

[65] Beispielsweise mit einer Monte Carlo-Simulation.

Risikohöhe: Ausmass des Risikos, geschätzt oder gemessen, als bestimmte Kombination von Auswirkungen und Eintrittswahrscheinlichkeit.

Risikoidentifikation: Prozess, um Risiken zu finden und mit ihren Ursachen und Auswirkungen zu beschreiben.

Risikokategorie: Eine Unterteilung der Risiken in thematische Gruppen.

Risikokommunikation: Andauernder oder wiederkehrender Prozess, um Informationen bezüglich des Umgangs mit Risiken mit den interessierten Parteien auszutauschen.

Risikokonsolidierung: Verfahren, das mehrere, unabhängig voneinander identifizierte Einzelrisiken aufgrund ihrer Art oder Bedeutung aggregiert, gruppiert oder selektioniert.

Risikokultur: Betriebsklima, in welchem alle Mitarbeitenden und jede Führungskraft einen bewussten Umgang mit Risiken und eine positive Fehlerkultur pflegen.

Risikomanagement-Prozess: Systematische Anwendung von Grundsätzen, Verfahren und Tätigkeiten, um über Risiken zu kommunizieren, Informationen auszutauschen, Zusammenhänge zu erstellen, Risiken zu identifizieren, zu analysieren, zu bewerten, zu bewältigen und zu überwachen.

Risikomanager: Person, die den Risikomanagement-Prozess auf Stufe Departement / BK anwendet und umsetzt sowie für die Einbettung des Risikomanagements im Departement / BK zuständig ist.

Risikopolitik: Absichten und Ziele des Bundesrates betreffend den Umgang mit Risiken. Die Risikopolitik wurde vom Bundesrat in der Form von verbindlichen Weisungen erlassen.

Risikorichtlinien: Verbindliche Vorgaben der EFV, wie das Risikomanagement in der Bundesverwaltung umzusetzen und laufend zu verbessern ist.

Risikoverminderung: Entscheidung über und Umsetzung von Massnahmen, um die Eintrittswahrscheinlichkeit oder die Auswirkungen eines Risikos günstig zu beeinflussen.

Szenario: Konkrete und bildhafte Darstellung eines Risikos mit Annahmen über mögliche Zusammenhänge von Ursachen und Abfolgen von Ereignissen oder Entwicklungen, die aufzeigt, wie sich Bedrohungen/Gefahren in der Bundesverwaltung verwirklichen können.

Top-down-Ansatz: Vorgehensweise bei der Risikobeurteilung, bei der die Gesamtheit der Organisation oder des Systems Gegenstand der Risikoidentifikation und -analyse ist.

Unerkanntes Risiko: Risiko einer Organisation, das trotz einer adäquaten Risikoidentifikation unerkannt bleibt und deshalb nicht bewirtschaftet werden kann.

Unsicherheit: Zustand fehlender Information bezüglich des Eintritts zukünftiger Ereignisse oder Entwicklungen, ihrer Auswirkungen und ihrer Wahrscheinlichkeit.

Value-at-Risk: Schadenhöhe, die bei einer bestimmten, genügend hohen Wahrscheinlichkeit (z. B. 95% oder 99%) nicht überschritten wird.

Verwaltungseinheit: Ämter der Bundesverwaltung. Sie besorgen die Verwaltungsgeschäfte.[66]

Wahrscheinlichkeit: Relative Häufigkeit des Eintritts zukünftiger Ereignisse oder Entwicklungen (objektive Definition). Unsicherheit von Aussagen bzw. Grad an persönlicher Überzeugung betreffend den Eintritt eines Ereignisses oder einer Entwicklung (subjektives Verständnis). Die Wahrscheinlichkeit eines Risikos kann sich auf eine Periode (z. B. Jahreswahrscheinlichkeit) oder auf eine Anzahl von Fällen (Fall-Wahrscheinlichkeit) beziehen.

Wechselwirkungen: Gegenseitige Abhängigkeiten oder Beeinflussungen zwischen einzelnen Risiken.

[66] Art. 43 Abs. 1 RVOG

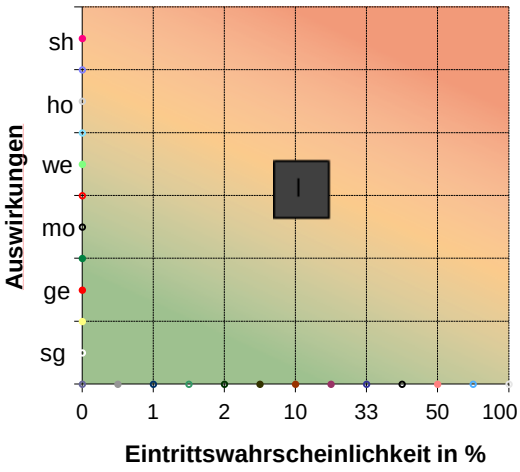
Anhang 2: Risikoerfassungsbogen

Risiko-Titel	
Abteilung/Bereich:	
Risikoeigner:	
Risikokategorie:	auswählen

Szenariobeschreibung (Ausgangslage (Ziel/Aufgabe) > Ursachen > Risiko > Auswirkungen (inkl. Wechselwirkungen)):

Ursachenbeschreibung (optional):

Bewertung:



Erläuterung Auswirkungen:

- *finanziell*:
- *Personenschäden*
- *Reputation:*
- *Geschäftsprozesse:*
- *Umwelt:*

Erläuterung Eintrittswahrscheinlichkeit:

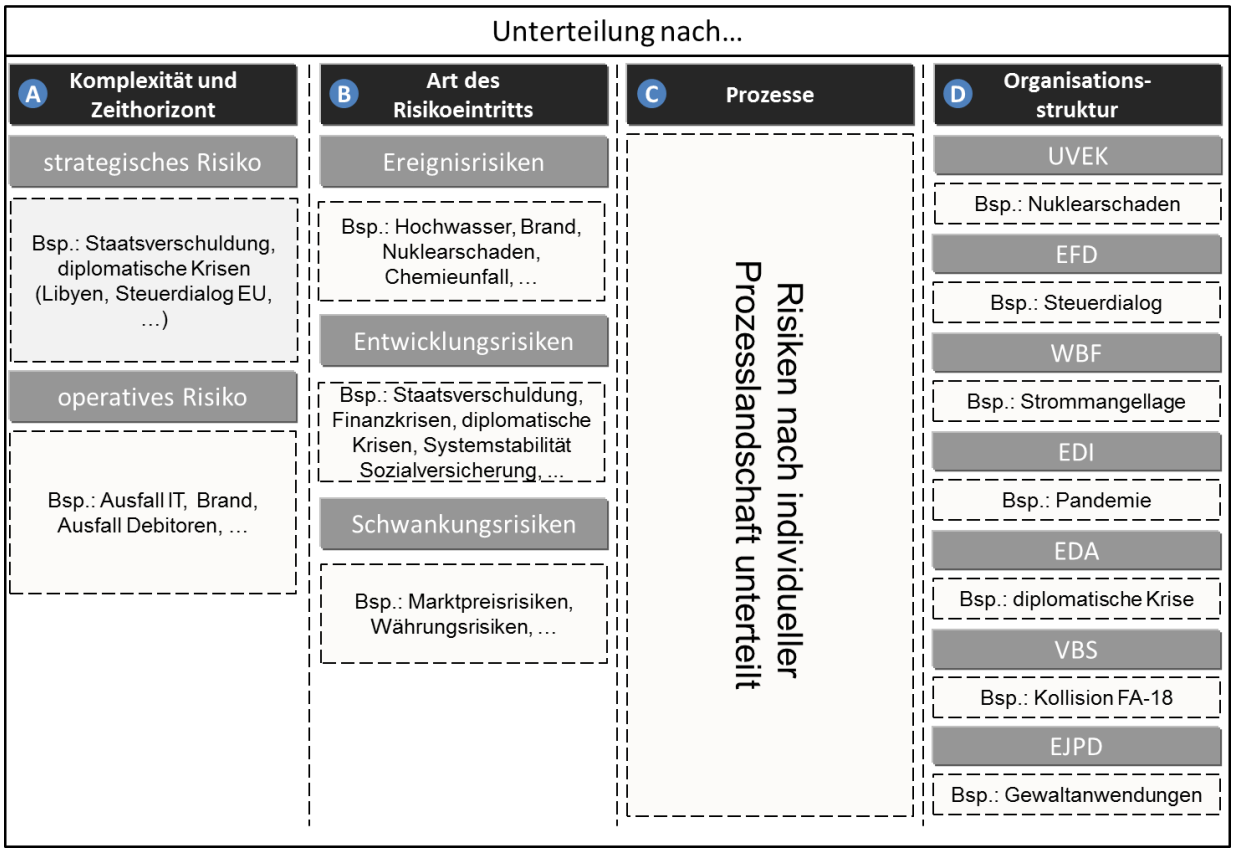
Erläuterung der Bewertungsänderung:

	Laufend durchgeführte, umgesetzte oder abgelehnte Massnahmen				***Status***
a.					
b.					
	neue Massnahmen in Planung (eingeleitet, beschlossen, möglich)	***wer***	***Termin***	***Kosten vs. Risikoreduktion (optional)***	***Status***
c.					
d.					
e.					
f.					

Datum: ..... Risikoeigner: ……

Anhang 3: Strukturierung von Risiken

Die folgenden Unterteilungen können neben den Risikokategorien zusätzlich hilfreich sein, um einen Überblick zu verschaffen und die Vielzahl an Risiken zu systematisieren. Dieser Abschnitt soll das gemeinsame Verständnis fördern und einen Anhaltspunkt geben, mit welchen Methoden das Risiko analysiert und bewertet werden kann.



a. ***Komplexität und Zeithorizont***: Eine Unterscheidung zwischen strategischen und operativen Risiken ist in der Theorie und Praxis vieler Organisationen üblich. Strategische und operative Risiken unterscheiden sich in mehrfacher Hinsicht: Strategische Risiken sind im Vergleich zu operativen Risiken meist komplexer (viele Zusammenhänge mit anderen Faktoren), längerfristiger Natur, abstrakter (weniger fassbar) und auf oberer Hierarchiestufe einer Organisation angesiedelt. Als weiteres Kriterium gilt manchmal auch die Höhe bzw. Bedeutung eines Risikos: grosse Risiken werden eher als strategisch bezeichnet und in die Verantwortung der obersten Hierarchiestufe angesiedelt. Zudem unterscheiden sich strategische Risiken häufig auch in der Art des Risikoeintritts von den operativen Risiken, indem sie häufig die Charakteristiken eines Entwicklungsrisikos aufweisen.

   Die Unterscheidung von strategischen und operativen Risiken erfolgt manchmal auch, um ein stufengerechtes Reporting zu erstellen: Während sich die Verantwortung auf oberster Hierarchiestufe eher auf die strategischen Risiken der Organisation konzentriert sind die tieferen Hierarchiestufen für das Management der operativen Risiken in ihrem Bereich verantwortlich.

Je nach Risikoart sind unterschiedliche Methoden für die Analyse und Bewertung zu verwenden: Bei strategischen Risiken bieten sich v.a. Indikator- und Szenarioanalysen an, bei operativen Risiken können je nach Risiko alle Methoden der Analyse Sinn machen. Die Methoden zur Analyse und Bewertung von Risiken werden in Ziffer 3.3.2 beschrieben.

b. ***Art des Risikoeintritts***: Risiken können in der Art unterschieden werden, wie sie auftreten. Bei einem *Ereignisrisiko* tritt dieses relativ schnell und plötzlich auf, meistens unerwartet. Ein *Entwicklungsrisiko* hingegen stellt eine Situation dar, die sich nach und nach verschärft und die negativen Auswirkungen im Zeitverlauf immer grösser werden, das Risiko ist also zeitlich nicht gut eingrenzbar und hat häufig einen längerfristigen Charakter. Ein solches Risiko kommt meistens auch nicht ganz unerwartet, weil es sich erst im Zeitverlauf entwickelt und durch Indikatoren schon vorher entdeckt werden kann. Die typische Eigenschaft eines *Schwankungsrisikos* ist, dass dieses eigentlich immer eintritt, wobei die Höhe und die Richtung des Ausschlags (Chance oder Risiko) vorher unbekannt sind. Finanzmarktrisiken sind typische Schwankungsrisiken.

   Je nach Art des Risikos sind unterschiedliche Methoden für die Analyse und Bewertung zu verwenden: Bei Schwankungsrisiken sind v.a. statistische Analysen sinnvoll, bei Ereignisrisiken am ehesten Szenarioanalysen und bei Entwicklungsrisiken machen Indikatoranalysen am meisten Sinn (vgl. Ziffer 3.3.2).

c. ***Prozesse***: Eine Unterteilung der Risiken nach Prozessen macht Sinn, wenn beispielsweise eine Verwaltungseinheit ein Qualitätsmanagement umsetzt und die Erfüllung ihrer Aufgaben mit Hilfe von klar definierten Prozessen steuert.

d. ***Organisationsstruktur***: Eine Unterteilung der Risiken nach Organisationsstruktur wird in der Praxis häufig umgesetzt. Eine solche Unterteilung unterstützt die klare Zuordnung eines Risikos zu einer Organisation und dessen Leitung.

Anhang 4: Pflichtenhefte für Risikomanager und Risikocoaches

Pflichtenheft Risikomanager

Umsetzen des Risikomanagementprozesses auf Stufe Departement / BK
▪ Zeitliche und organisatorische Planung und Kommunikation des Risikomanagementprozesses auf Stufe Departement / BK in Abstimmung mit den Terminen der Koordinationsstelle EFV. ▪ Durchführen des Risikomanagementprozesses in der Funktion als Risikocoach im Generalsekretariat (Fokus auf Aufgaben des Departements / der BK).
Einheitliches Implementieren des Risikomanagements innerhalb des Departements / der BK
▪ Abklären des Bedarfs nach einer departementsweiten Risikorichtlinie, welche die Vorgaben aus der Risikorichtlinie Bund berücksichtigt und allfälliges Erstellen einer Richtlinie auf Stufe Departement / BK.
Koordination und Steuerung der Risikocoaches der VE des Departements.
▪ Organisiert den fachlichen Austausch der Risikocoaches innerhalb des Departements mit regelmässigen Sitzungen. ▪ Organisiert und führt die Abstimmung bezüglich Querschnittsrisiken innerhalb des Departements.
Erstellen des Risikoreportings auf Stufe Departement / BK
▪ Zusammenführen der aus den VE (inkl. Generalsekretariat) gemeldeten Departementsrisiken, Prüfung von Wechselwirkungen zwischen den Risiken. ▪ Analyse und Führen der Diskussionen, Abklärungen und des Quervergleichs der Departementsrisiken innerhalb des Departements / der BK und zwischen den VE. ▪ Erstellen eines Reportings für den Departementsvorsteher und die Leitung des Departements / der BK. ▪ Zustellen des Reportings an die Koordinationsstelle EFV für das Bundesratsreporting. ▪ Vorschlag bezüglich Auswahl der Kernrisiken des Departements / der BK (Entscheid beim Vorsteher).
Koordinieren die Abstimmungen zur Analyse von Wechselwirkungen zwischen Risiken aus unterschiedlichen VE
Fachliche Unterstützung der Risikoeigner auf Stufe Departement / BK und der Risikocoaches
▪ Antworten auf Fragen zur Methodik des Risikomanagements der Risikoeigner auf Stufe Departement / BK. ▪ Antworten auf Fragen zum System R2C und fachlichen Fragen der Risikocoaches.
Schnittstelle zur und Ansprechperson für die Koordinationsstelle EFV
▪ Teilnahme an den regelmässigen Risikomanagement-Workshops auf Stufe Bund (organisiert durch die Koordinationsstelle EFV). ▪ Zusammenarbeit mit Koordinationsstelle EFV bei der Diskussion der Bundesratsrisiken des Departements / der BK.
Entscheide des BR, der GSK und der Koordinationsstelle EFV den Risikocoaches und den Risikoeigner stufengerecht kommunizieren.
Vernetzung des Risikomanagements mit anderen Führungsprozessen im Departement / in der BK.
Vernetzen des Risikomanagements mit weiteren Führungsprozessen, insb. mit dem IKS, mit dem Qualitätsmanagement, dem IT-Sicherheitsmanagement usw.

Verbesserung des Risikomanagements im Departement / in der BK und in der Bundesverwaltung
▪ Aus den Erfahrungen im Risikomanagement Ideen generieren, um das Risikomanagement in der Bundesverwaltung zu verbessern und weiterzuentwickeln. ▪ Teilnahme an Risikomanagement-Veranstaltungen, insb. bei Veranstaltungen mit thematischem Bezug zum Departement / zur BK. ▪ Fördern des Risikobewusstseins auf Stufe Departement / BK und im Generalsekretariat.

Pflichtenheft Risikocoach

Umsetzung Risikomanagementprozess auf Stufe VE
▪ Zeitliche und organisatorische Planung und Kommunikation des Risikomanagementprozesses innerhalb der VE in Abstimmung mit den Terminen auf Stufe Departement (Vorgabe des Risikomanagers). ▪ Durchführung des Risikomanagementprozesses in der VE: Gruppen-Workshops mit Leitung der VE bzw. geeigneten Wissensträgern, Einzeldiskussionen usw.
Einheitliche Implementierung des Risikomanagements innerhalb der VE
▪ Abklärung des Bedarfs nach einer VE-spezifischen Risikorichtlinie, welche die Vorgaben aus der Risikorichtlinie Bund bzw. Departement berücksichtigt.
Erstellen eines adäquaten Risikoreportings auf Stufe VE
▪ Zusammenführen der in den Abteilungen und Sektionen erfassten und analysierten Risiken inkl. der vorgeschlagenen Massnahmen. ▪ Führen der Diskussionen, Abklärungen und des Quervergleichs zwischen den Risiken der unterschiedlichen Abteilungen. ▪ Erstellen eines Reportings für den Leiter der VE. ▪ Erstellen eines Reportings für den Risikomanager des Departements.
Fachliche Unterstützung der Risikoeigner auf Stufe VE
▪ Antworten auf Fragen zur Methodik des Risikomanagements und Strukturierung von Risiken der Risikoeigner und der Direktion der VE.
Schnittstelle zur und Ansprechperson für den Risikomanager des Departements
▪ Teilnahme an Risikomanagementsitzungen im Departement (organisiert durch den Risikomanager). ▪ Zusammenarbeit und Austausch bezüglich Auswahl der Departementsrisiken der VE.
Entscheide des BR, der GSK, der Koordinationsstelle EFV und des Risikomanagers der Direktion der VE und den Risikoeigner der VE stufengerecht kommunizieren.
Vernetzung des Risikomanagements mit anderen Führungsprozessen in der VE
▪ Vernetzen des Risikomanagements mit weiteren bestehenden Führungsprozessen in der VE, insb. mit dem IKS, aber auch mit dem Qualitätsmanagement, dem IT-Sicherheitsmanagement usw.
Verbesserung des Risikomanagements in der VE und in der Bundesverwaltung
▪ Aus den Erfahrungen im Risikomanagement Ideen generieren, um das Risikomanagement in der VE und in der Bundesverwaltung zu verbessern und weiterzuentwickeln. ▪ Teilnahme an Risikomanagement-Veranstaltungen, insb. bei Veranstaltungen mit thematischem Bezug zur VE. ▪ Fördern des Risikobewusstseins innerhalb der VE.

Anhang 5: Beispiel einer Einsichtsverweigerung in das Risikomanagement Bund (konkret: in die Risikodatenbank R2C)

Einschreiben
xxx
xxx
xxx

Bern, xxx

Ihr Einsichtsgesuch vom xxx

Sehr geehrter Herr xxx

Mit E-Mail vom xxx verlangten Sie von der EFV gestützt auf das Öffentlichkeitsgesetz (BGÖ; SR *152.3*) Einsicht in die «Datenbank R2C (Risikomanagementsystem zur Erfassung der bundesweiten Risiken)».

Nach Prüfung der Sachlage gelangen wir zu folgender ***Stellungnahme***:

1. Der Zugang wird verweigert.
2. Eine Gebühr wird nicht erhoben (Art. 17 Abs. 2 Bst. a BGÖ).

Begründung:
Die EFV stellt den Departementen / der BK für die Bewirtschaftung ihrer Risiken und die Risikoberichterstattung eine gemeinsame Informatikanwendung zur Verfügung. Die Kurzbezeichnung der Anwendung lautet «R2C». Die wesentlichen Risiken des Bundes werden darin im Detail identifiziert, analysiert und bewertet. Ausserdem werden Massnahmenpläne inklusive deren Stand der Umsetzung dargelegt. Die Risikoberichterstattung erfolgt (mindestens) einmal jährlich und wird auf allen Stufen (VE, Departement / BK, Generalsekretärenkonferenz, Bundesrat) als VERTRAULICH klassifiziertes Geschäft behandelt. Zwecks Wahrung der Vertraulichkeit der Informationen haben auch die Geschäftsprüfungskommissionen für die Behandlung der Risikoberichterstattung an den Bundesrat besondere Massnahmen getroffen.

Die Klassifizierungsstufe wurde aufgrund des vorliegenden Gesuchs überprüft (Art. 11 Abs. 5 Öffentlichkeitsverordnung [SR *152.31*] i.V.m. Art. 13 Abs. 3 Informationsschutzverordnung [SR *510.411*]); sie ist gerechtfertigt.

Das Interesse des Bundes an der Wahrung der Vertraulichkeit der in der Applikation R2C aufgeführten Informationen ist gross. Eine Einsichtnahme könnte insbesondere die freie Meinungs- und Willensbildung in Bezug auf die Bewirtschaftung der Risiken und die zu treffenden Massnahmen beeinträchtigen. Ausserdem besteht die Gefahr der Vereitelung der zielkonformen Durchführung von konkreten behördlichen Massnahmen und auch die innere und äussere Sicherheit der Schweiz könnte unter Umständen erheblich gefährdet sein.

Ein höher zu gewichtendes Interesse an der Einsichtnahme ist vorliegend nicht ersichtlich.

Aus diesen Gründen wird der Zugang zu den in R2C enthaltenen Informationen insbesondere gestützt auf Art. 7 Abs. 1 Bst. a–c BGÖ nicht gewährt.

Freundliche Grüsse

xxx
Öffentlichkeitsverantwortliche EFV

Hinweis auf das Schlichtungsverfahren (vgl. Art. 13 BGÖ)

[1] *Einen Schlichtungsantrag stellen kann eine Person:*

a. deren Zugang zu amtlichen Dokumenten eingeschränkt, aufgeschoben oder verweigert wird;

b. zu deren Gesuch die Behörde nicht fristgerecht Stellung genommen hat; oder

c. die nach Artikel 11 angehört worden ist, wenn die Behörde gegen ihren Willen den Zugang gewähren will.

[2] *Der Schlichtungsantrag ist der oder dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten innert 20 Tagen nach Empfang der Stellungnahme oder nach Ablauf der der Behörde für die Stellungnahme zur Verfügung stehenden Frist schriftlich zu stellen.*

Anhang 6: Schnittstelle «Risikomanagement – Rechnungslegung» im Bund

<table>
<tr><th rowspan="2">Verpflichtung</th><th rowspan="2">Eintrittswahr-scheinlichkeit</th><th rowspan="2">Wahrscheinlich-keit des Mittel-ab-flusses</th><th colspan="2">Jahresrechnung des Bundes</th><th rowspan="2">Risiko-management</th></tr>
<tr><th>Begriffe[67]</th><th>Ausweis</th></tr>
<tr><td rowspan="3">bestehende</td><td>–</td><td>voraussehbar
(100 %)[68]</td><td>Verpflichtung
(Art. 49 Abs. 2 FHG)</td><td rowspan="2">Passivierung in der Bilanz
(Art. 56 FHV)</td><td>kein Ausweis</td></tr>
<tr><td>–</td><td>überwiegend wahrscheinlich
(50–100 %)</td><td>Rückstellung
(Art. 49 Abs. 3 FHG)</td><td rowspan="4">Ausweis in der Riskmap
(Art. 50 FHV)</td></tr>
<tr><td>–</td><td>eher unwahr-scheinlich
(10–50 %)</td><td rowspan="2">Eventual-verbindlichkeit
(Art. 3 Bst. d FHV)</td><td rowspan="2">Offenlegung im An-hang zur Jahres-rechnung
(Art. 3 Bst. d FHV)</td></tr>
<tr><td rowspan="2">künftige</td><td>ungewiss aber möglich
(10–100 %)</td><td>–</td></tr>
<tr><td>sehr unwahr-scheinlich
(0–10 %)</td><td>–</td><td>–</td><td>Verweisung im An-hang zur Jahres-rechnung
(Art. 3 Bst. b FHV)</td></tr>
</table>

[67] vgl. Botschaft vom 24. November 2004 zur Totalrevision des Bundesgesetzes über den eidgenössischen Finanzhaushalt (BBl *2005* 5, S. 15, 57, 61 f., 85 f., 104 f. und 107).

[68] Ein Mittelabfluss ist *voraussehbar* nach Art. 49 Abs. 2 FHG (Kurzformel: Wahrscheinlichkeit = 100%), wenn sein Eintritt *praktisch sicher* ist. Hingegen kann es keine *absolute Gewissheit* für ein in der Zukunft liegendes Ereignis geben.

Anhang 7: Organisationen ausserhalb der Bundesverwaltung

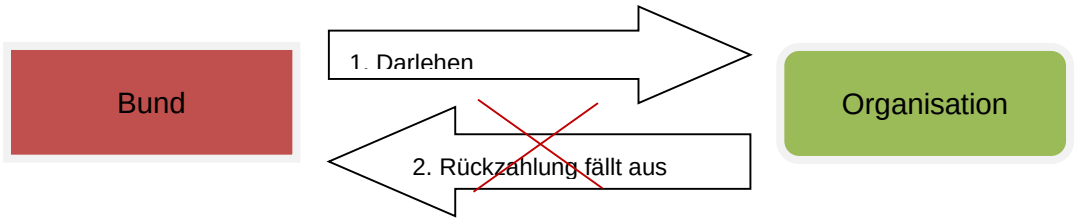
Durch Gesetze und andere Verknüpfungen trägt der Bund in speziellen Fällen Risiken aus Organisationen, die ausserhalb der Bundesverwaltung stehen. Das Risiko des Bundes hängt davon ab, in was für einer Beziehung der Bund zur fraglichen Organisation steht. Ohne Anspruch auf Vollständigkeit können folgende Konstellationen erwähnt werden:

1. Der Bund gewährt einer Organisation z. B. ein Darlehen, eine Bürgschaft, eine (Ausfall-)Garantie usw.
2. Der Bund übt gegenüber einer Organisation eine Aufsichtsfunktion aus oder es obliegt ihm (bzw. der EFK), als Revisionsstelle der Organisation zu amten.
3. Einer Organisation, die rechtlich und finanziell ausserhalb der Bundesverwaltung steht, ist mittels gesetzlicher Vorschrift die Erfüllung einer öffentlich-rechtlichen Aufgabe des Bundes übertragen und den Bund trifft in der Folge eine Ausfallhaftung.
4. Der Bund entsendet Vertreter in Leitungs- oder Verwaltungsorgane einer Organisation.
5. Der Bund haftet aus fusionsrechtlichen Vorgängen z. B. bei der Ausgliederung einer Einheit aus der Bundesverwaltung.
6. Die Beteiligungen des Bundes an einer ausgegliederten Einheit können an Wert verlieren oder diese Einheit liefert dem Bund als Eigner weniger Gewinn ab.

Auf diese Konstellationen soll hiernach aus der Optik Risikomanagement Bund etwas näher eingegangen werden.

1. Darlehen, Bürgschaften, Garantien usw.

Darlehen: Der Bund gewährt einer ausserhalb der zentralen Bundesverwaltung stehenden Organisation ein Darlehen. Die Organisation kann das Darlehen nicht zurückzahlen.



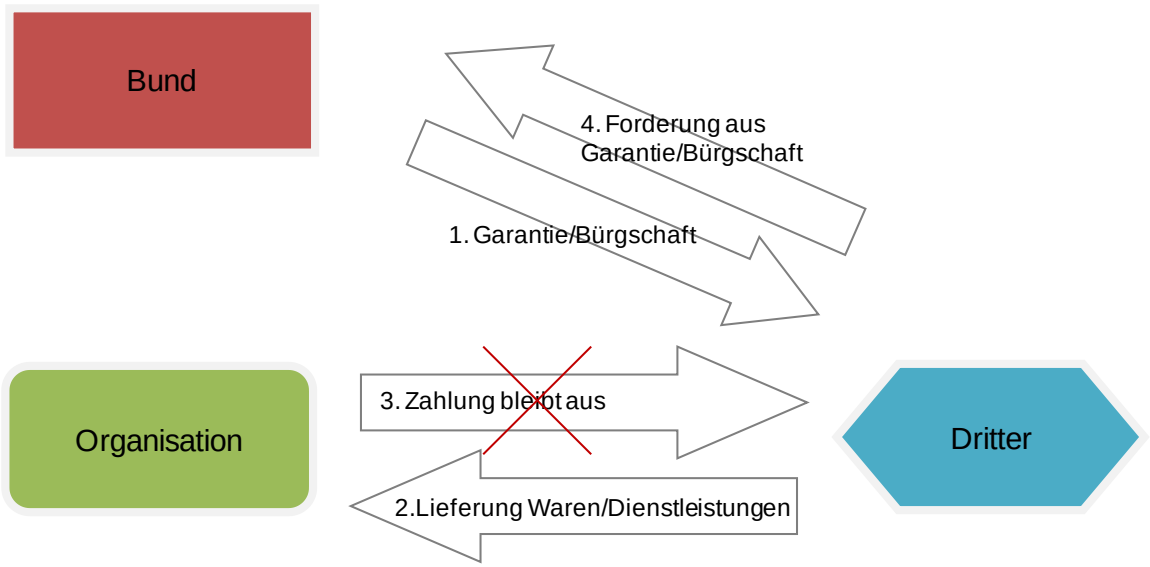
Beispiele:

- Darlehen an Transportunternehmen zur Finanzierung von Fahrzeugen und Einrichtungen[69].
- Darlehen an Einheiten der dezentralen Bundesverwaltung zur Sicherstellung der Liquidität[70].

Garantien und Bürgschaften: Der Bund garantiert für Verpflichtungen von ausserhalb der Bundesverwaltung stehenden Organisationen gegenüber Dritten oder stellt eine Bürgschaft.

[69] Z. B. Art. 34 Abs. 2 des Personenbeförderungsgesetzes vom 20. März 2009 (PBG; SR 745.1); Art. 14 des Alpentransit-Gesetzes vom 4. Oktober 1991 (AtraG; SR 742.104).
[70] Z. B. Art. 18 Abs. 2 des Museums- und Sammlungsgesetzes vom 12. Juni 2009 (MSG; SR 432.30); Art. 28 Abs. 1 des Exportrisikoversicherungsgesetzes vom 16. Dezember 2005 (SERVG; SR 946.10).

Die Organisation kommt ihren Verpflichtungen nicht nach. Der Dritte greift auf den Bund zu. In der Regel kann er dies erst, wenn er von der Organisation erfolglos Erfüllung verlangt hat.



Beispiele:

- Staatsgarantien: z. B. Garantien zu Gunsten von Transportunternehmen für Investitionen im Verkehrsbereich[71]; Staatsgarantie zu Gunsten der Schweizerischen Post[72] und den SBB für deren Verbindlichkeiten gegenüber «Eurofima»[73].
- Garantie, die ständige Zahlungsbereitschaft von Einheiten der dezentralen Bundesverwaltung ohne eigene Rechnung sicherzustellen[74].
- Bürgschaften: z. B. für Anleihensobligationen gemeinnütziger Emissionszentralen oder Rückbürgschaften für Bürgschaften von Hypothekar-Bürgschaftseinrichtungen zur Finanzierung von preisgünstigen Mietwohnungen an Träger des gemeinnützigen Wohnungsbaus[75].
- Faktische Staatsgarantien an systemrelevante Unternehmen (z. B. des Finanzsektors[76]).

Vereinzelt ist der Bund auf Grund eines Gesetzes verpflichtet, ausserhalb der Bundesverwaltung stehende Organisationen zu refinanzieren. Beispiel: Refinanzierung des Fehlbetrages in der Pensionskasse der SBB[77].

---

[71] Art. 34 Abs. 1 PBG.
[72] Gesamtschau zur weiteren Entwicklung des Postwesens in der Schweiz – Bericht des Bundesrates und Botschaft über die Änderung des Postorganisationsgesetzes vom 22. Mai 2002, BBl. *2002* 5077; Botschaft vom 20. Mai 2009 zum Bundesgesetz über die Organisation der Schweizerischen Post (Postorganisationsgesetz, POG), BBl. *2009* 5287 f.
[73] Art. 5 des Abkommens vom 20. Oktober 1955 über die Gründung der «Eurofima», Europäische Gesellschaft für die Finanzierung von Eisenbahnmaterial (SR 0.742.105).
[74] Art. 60 Abs. 1 des Finanzhaushaltgesetzes vom 7. Oktober 2005 (FHG; SR 611.0).
[75] Art. 35 und 36 des Wohnraumförderungsgesetzes vom 21. März 2003 (WFG; SR 842).
[76] siehe: Botschaft vom 20. April 2011 zur Änderung des Bankengesetzes (Stärkung der Stabilität im Finanzsektor; *too big to fail*), BBl. *2011* 4727.
[77] Art. 16 Abs. 4 des Bundesgesetzes vom 20. März 1998 über die Schweizerischen Bundesbahnen (SBBG; SR 742.31).

2. Aufsichts- oder Revisionstätigkeit des Bundes

Ein Angestellter des Bundes vernachlässigt die Aufsicht über eine ausserhalb der Bundesverwaltung stehende Organisation[78]. Ein Dritter kommt zu Schaden. Sofern die gesetzlichen Voraussetzungen erfüllt sind, haftet der Bund für den Schaden des Dritten[79].

Die EFK kann als Revisionsstelle von ausserhalb der Bundesverwaltung stehenden Organisationen eingesetzt sein[80]. Verursacht die EFK durch Verletzung ihrer Pflichten als Revisionsstelle einen Schaden und sind die weiteren Voraussetzungen einer besonderen Haftungsnorm[81] erfüllt, kann der Bund zu Schadenersatz verpflichtet werden.

3. Ausfallhaftung des Bundes nach Art. 19 Verantwortlichkeitsgesetz (VG)

Ein Angestellter oder ein Organ einer ausserhalb der Bundesverwaltung stehenden Organisation mit eigener Rechtspersönlichkeit und eigener Rechnung, die per Bundesgesetz mit der Erfüllung einer öffentlichen Aufgabe betraut ist, fügt einem Dritten in Ausführung dieser Aufgabe widerrechtlich Schaden zu. Das Vermögen der Organisation reicht nicht aus, um den Schaden zu decken. Der Bund muss subsidiär für den Schaden einstehen.[82]

---

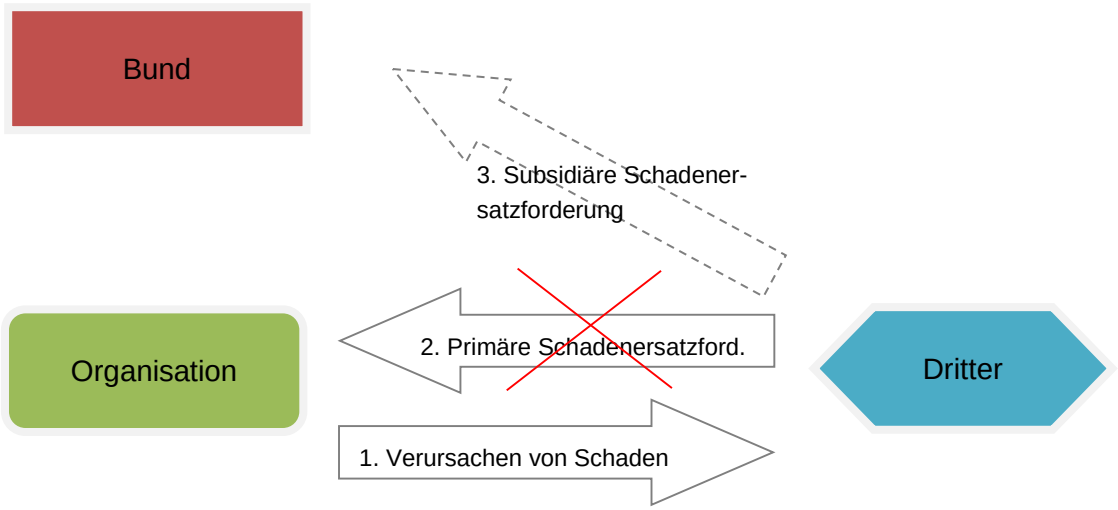
78 Z. B. Aufsicht des BAV über den Bau und Betrieb von Eisenbahnen (Art. 10 des Eisenbahngesetzes vom 20. Dezember 1957 [EBG; SR 742.10]) oder die Personenbeförderung im öffentlichen Verkehr (Art. 52 PBG) sowie Kontrolle der Einhaltung der internationalen Normen, der gesetzlichen Vorschriften und der Konzessionsbestimmungen im Fernmeldewesen durch das BAKOM (Art. 58 des Fernmeldegesetzes vom 30. April 1997 [FMG: SR 784.10]).

79 Massgebend ist Artikel 3 des Verantwortlichkeitsgesetzes vom 14. März 1958 (VG; SR 170.32).

80 Z. B. revidiert die EFK die Rechnungen des ETH-Bereichs (Art. 35*a* Abs. 3 des ETH-Gesetzes vom 4. Oktober 1991 [SR 414.110]), der FINMA (Art. 12 des Finanzmarktaufsichtsgesetzes vom 22. Juni 2007 [FINMAG; SR 956.1]) und der Revisionsaufsichtsbehörde (Art. 32 des Revisionsaufsichtsgesetzes vom 16. Dezember 2005 [RAG; SR 221.302).

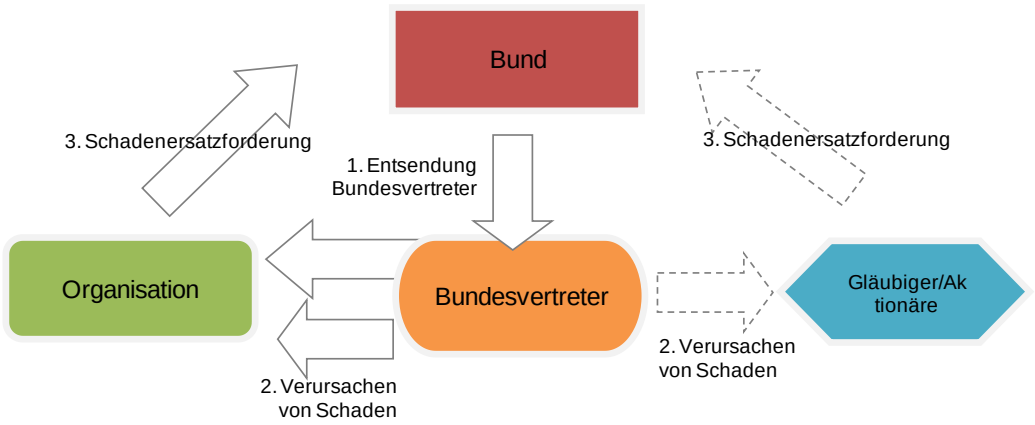
81 Amtet die EFK als Revisionsstelle von öffentlich-rechtlichen Anstalten oder Stiftungen richtet sich die Haftung grundsätzlich nach Art. 3 VG (siehe dazu Fn. 79). Wäre die EFK als Revisionsstelle privatrechtlicher Aktiengesellschaften eingesetzt, würde der Bund nach Art. 755 Abs. 2 OR haften. Anders als bei Art. 3 VG müsste der EFK in diesem Fall ein Verschulden vorzuwerfen sein.

82 Art. 19 Abs. 1 Bst. a VG.



4. Haftung für entsandte Bundesvertreter

Die Statuten von Aktiengesellschaften können vorsehen, dass der Bund einen Vertreter in den Verwaltungsrat entsenden kann[83]. Der Bund haftet gegenüber der Gesellschaft, den Aktionären und den Gläubigern, wenn der Vertreter durch absichtliche oder fahrlässige Verletzung seiner Pflichten einen Schaden verursacht[84].



[83] Art. 762 Abs. 1 OR.
[84] Art. 762 Abs. 4 OR. Das Verhalten des Bundesvertreters muss eine besondere Haftungsnorm erfüllen (z. B. Art. 754 OR). Insbesondere muss ihm ein Verschulden vorzuwerfen sein. Ähnliches gilt für Genossenschaften (vgl. Art. 926 Abs. 4 OR)

5. Haftung für fusionsrechtliche Vorgänge

Fusioniert eine im Handelsregister eingetragene, organisatorisch verselbständigte Einheit des öffentlichen Rechts mit einer privatrechtlichen Einheit[85] oder wandelt sich in eine privatrechtliche Einheit um[86], muss der Bund Vorkehrungen zum Schutz der Gläubiger treffen. Sind diese Vorkehren[87] ungenügend, haftet der Bund[88].

6. Verluste auf Beteiligungen und Unterstützungsmassnahmen

Der Bund ist gesetzlich verpflichtet, Beteiligungen an ausserhalb der Bundesverwaltung stehenden Organisationen zu halten[89] oder er hält solche Beteiligungen aufgrund subventionsrechtlicher Bestimmungen[90]. Durch innere und äussere Einflüsse können diese Beteiligungen an Wert verlieren, was sich in der Rechnung des Bundes zeigt und eine direkte finanzielle Auswirkung zur Folge hat. Weiter könnte der Bund verpflichtet sein, bei solchen Beteiligungen Unterstützungsmassnahmen zu leisten, wenn die gesetzlich übertragene Aufgabenerfüllung nicht mehr gewährleistet ist.

[85] Das Gesetz bezeichnet die zulässigen Fusionen: Zulässig ist die Übernahme einer öffentlich-rechtlichen Einheit durch eine Kapitalgesellschaft, eine Genossenschaft, einen Verein oder eine Stiftung (Absorption) sowie Formen der Kombinationsfusion, an der mindestens eine öffentlich-rechtliche Einheit beteiligt ist und aus der eine Kapitalgesellschaft, eine Genossenschaft, ein Verein oder eine Stiftung hervorgehen (Art. 99 Abs. 1 Bst. a des Fusionsgesetzes vom 3. Oktober 2003 [FusG; SR 221.301]). Nicht zulässig ist die Absorption einer privatrechtlichen Einheit durch eine öffentlich-rechtliche Einheit (Botschaft vom 13. Juni 2000 zum Bundesgesetz über Fusion, Spaltung, Umwandlung und Vermögensübertragung, BBl. 2000 4481). Spezialgesetzliche Aktiengesellschaften (z. B. die SBB) gelten als öffentlich-rechtliche Einheiten (BGE 132 III 470, 478 f.).

[86] Öffentlich-rechtliche Einheiten können sich in Kapitalgesellschaften, Genossenschaften, Vereine oder Stiftungen umwanden (Art. 99 Abs. 1 Bst. b FusG).

[87] Als Mindeststandard müssen Artikel 26 und 68 Absatz 1 FusG bezüglich Inhalt, Umfang und Dauer in einer dem öffentlichen Recht angepassten Form gewährleistet sein. Nicht zwingend ist, dass es sich dabei um Nachhaftungen der öffentlichen Hand handelt (Botschaft FusG [Fn. 85], 4484.

[88] Art. 101 FusG.

[89] Art. 7 Abs. 3 SBBG; Art. 6 Abs. 1 des Telekommunikationsunternehmensgesetzes vom 30. April 1997 (TUG; SR 784.11).

[90] Bsp. Art. 38 WFG.

Anhang 8: Projekte mit Bezug zum Risikomanagement

Im folgenden Anhang werden aktuelle mittlere und grosse Projekte in der Bundesverwaltung vorgestellt, die sich mit konkreten Themen des Risikomanagements auseinandersetzen. Neben einer kurzen Erläuterung sollen vorhandene Schnittstellen und die Zusammenarbeit mit dem Risikomanagement Bund aufgezeigt werden.

I. Schutz kritischer Infrastrukturen

Das übergeordnete Ziel im Bereich Kritische Infrastrukturen ist es, grossflächige Ausfälle von Kritischen Infrastrukturen zu verhindern respektive das Schadensausmass bezüglich Raum, Zeit und Intensität im Falle von Störungen zu reduzieren. Obwohl sich in einzelnen Bereichen die verantwortlichen Stellen auf Stufe Bund, Kantone, Betreiber mit Aspekten zur Erfüllung des Zieles beschäftigen, fehlte bis anhin eine übergreifende Koordination. Im Auftrag des Bundesrates erarbeitet deshalb das Bundesamt für Bevölkerungsschutz (BABS) im Projekt «Schutz Kritischer Infrastrukturen» (SKI) eine nationale, übergreifende Koordination und ein einheitliches Vorgehen im Bereich der Kritischen Infrastrukturen.

Während sich Risikomanagement Bund auf die Risiken für die Bundesverwaltung konzentriert, fokussiert das Projekt auf Risiken für die Kritischen Infrastrukturen. Dabei ergeben sich verschiedene Schnittstellen, da 1) die Bundesverwaltung auch Teil des kritischen Sektors Behörden ist, 2) ein Ausfall von Kritischen Infrastrukturen auch schwerwiegende Auswirkungen auf die Bundesverwaltung haben kann, 3) der Bund teilweise und vollumfänglich Unternehmen aus verschiedenen kritischen Sektoren besitzt und schliesslich 4) der Bund in gewissen Bereichen verantwortlich für die Sicherstellung der Funktionsfähigkeit von Kritischen Infrastrukturen (z.B. in der Stromversorgung) ist, womit ein entsprechender Ausfall auch Rückwirkungen auf den Bund haben könnte.

Das Risikomanagement Bund ist im Projekt SKI mit einbezogen und stellt sicher, dass Risiken aus Sicht Bundesverwaltung und weitere Erkenntnisse in das bundesverwaltungsweite Risikomanagement einfliessen. Weiter unterstützt es das Projekt mit Erkenntnissen und Know-how aus dem Risikomanagement Bund.

II. Nationale Gefährdungsanalyse

Die Nationale Gefährdungsanalyse untersucht die Auswirkungen von verschiedenen Gefährdungen aus den Bereichen Natur, Technik und Gesellschaft auf Bevölkerung, Wirtschaft, Umwelt und gesellschaftliche Errungenschaften in der Schweiz. Übergeordnetes Ziel ist es, eine gemeinsame Grundlage zur Vorbereitung der Gesellschaft auf die Bewältigung von bestimmten Schadensereignissen zu schaffen. Ein gemeinsames Verständnis über die verschiedenen Auswirkungen, den Ablauf und die Dynamik von Gefährdungen ist dabei zentral, weil (die Vorbereitung auf) deren Bewältigung eine immer engere Zusammenarbeit verschiedener Stellen bei Bund und Kantonen, der Wirtschaft, Wissenschaft und Bevölkerung erfordert. Die *Nationale Gefährdungsanalyse von Katastrophen und Notlagen in der Schweiz* wurde vom Bundesrat in Auftrag geben und wird im Bundesamt für Bevölkerungsschutz koordiniert. Im Rahmen der Arbeiten zur nationalen Gefährdungsanalyse wurden mehrere Produkte entwickelt, die periodisch aktualisiert werden, dazu zählen[91]:

- Der Risikobericht (zeigt die Resultate der Analysen von 33 untersuchten Katastrophenereignissen und Notlagen und wie diese zueinander

[91] Vgl. auch http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/gefaehrdungen-risiken/nat__gefaehrdungsanlayse.html

in Beziehung stehen).
- Methode (Dokumentation des Vorgehens und der angewandten Metrik in der nationalen Gefährdungsanalyse).
- Gefährdungskatalog (Zusammenstellung möglicher Gefährdungen. Der Katalog stellt eine Übersicht denkbarer Ereignisse und Entwicklungen dar, ohne diese zu priorisieren).
- Gefährdungsdossiers (zu den identifizierten Gefährdungen werden vorhandene Informationen aufgearbeitet, systematisch aufgebaute Szenarien entwickelt und in einem sogenannten Gefährdungsdossier zusammengestellt. Die Szenarien in den Gefährdungsdossiers sind die Grundlage für die Risikoanalyse bzw. den Risikobericht).

Während sich Risikomanagement Bund auf die Bundesverwaltung konzentriert, fokussieren sich die Arbeiten im Rahmen der nationalen Gefährdungsanalyse auf Katastrophen und Notlagen mit Auswirkungen auf die Bevölkerung und ihre Lebensgrundlagen.

Anhang 9: Stolpersteine im Risikomanagement

Einige allgemeine Stolpersteine, die eine effektive Umsetzung des Risikomanagements insbesondere bei komplexen und schwer fassbaren Risiken beeinträchtigen können und eine allmähliche Entwicklung von Risiken begünstigen können, werden nachfolgend kurz erläutert.[92] Es ist Aufgabe der Risikoeigner, der Risikomanager und Risikocoaches, solche Probleme in ihrem Bereich zu identifizieren und zu minimieren.

- ***Bürokratie:*** Eine proaktive Umsetzung des Risikomanagementprozesses ist für den Erfolg entscheidend. Nachdem der Prozess einige Jahre immer gleich durchgespielt und umgesetzt wurde, steigt die Gefahr, dass er danach immer mehr zu einer bürokratischen Routinearbeit verkommt. Dies führt dazu, dass nicht mehr proaktiv nach neuen Risiken und Änderungen der bestehenden Risiken gesucht, der Prozess möglichst rasch und ohne ein entsprechendes Engagement durchgeführt und so wichtige Risiken nicht erkannt und keine entsprechenden Gegenmassnahmen getroffen werden.

- ***Fehlender Einbezug von Anspruchsgruppen:*** Der Einbezug aller relevanten Personen im Risikomanagementprozess ist von grosser Bedeutung. Erstens stellt er sicher, dass die bestmögliche und möglichst vollständige Information zur objektiven Beurteilung eines Risikos vorliegt. Zweitens hilft er, das Vertrauen (intern und extern) in das Risikomanagement und dessen Resultate wesentlich zu erhöhen. Ein fehlender Anspruchsgruppeneinbezug kann schliesslich zu erheblichen Verzögerungen in der Analyse und Bewältigung von Risiken führen.
  Beispiel: grosse Kraftwerksprojekte (breit angelegter Einbezug von Anspruchsgruppen ermöglicht erst deren Umsetzung)

- ***Interessenkonflikte und absichtliche Fehldarstellung von Risiken***: Sowohl bei der Analyse von Risiken als auch bei der Umsetzung von Bewältigungsmassnahmen können vorhandene Interessenkonflikte den Risikomanagementprozess behindern. Spezifische Interessen von Anspruchsgruppen können einerseits zu einer absichtlichen oder unabsichtlichen Fehldarstellung und -analyse von Risiken führen. Andererseits können sie auch notwendige Massnahmenumsetzungsentscheide blockieren.

[92] Die hier vorgestellten und weitere Strukturen und Eigenheiten werden im Report der IRGC ‚Risk governance deficits' genauer erläutert, vgl. http://www.irgc.org/-Risk-Governance-Deficits-.html

Interessenkonflikte müssen aufgedeckt und wenn möglich gelöst werden.
Beispiel: von der Tabakindustrie finanzierte Studien über gesundheitliche Risiken des Rauchens

- ***Verstreute bzw. nicht klar geregelte Verantwortlichkeiten***: Besonders in komplexen Organisationen, in denen verschiedene Akteure gemeinsam Verantwortung tragen oder die Verantwortung nicht klar geregelt ist, kann dies in Kombination mit einer schlechten Kommunikation dazu führen, dass notwendige Massnahmenentscheide nicht oder zu spät gefällt und umgesetzt werden, weil niemand voll in der Verantwortung steht.
  Beispiel: Strom-Blackout Italien

- ***Abwägung zwischen Transparenz und Vertraulichkeit:*** Die Vertraulichkeit (und damit die fehlende Kommunikation) von Risikoinformationen ist in einigen Fällen zum Schutz der nationalen Sicherheit oder zur Vermeidung von öffentlicher Panik gerechtfertigt. Fehlende Transparenz bezüglich Risiken kann andererseits das Vertrauen in das Risikomanagement vermindern und aufgrund fehlender Informationen dazu führen, dass einige Risiken deswegen nicht die nötige Dringlichkeit zu ihrer Bewältigung erhalten.
  Beispiel: Bilanzfälschung Enron

- ***Informationsasymmetrien:*** In einigen Fällen dient die Aufrechterhaltung von Informationsasymmetrien den Zielen des Risikomanagements, beispielsweise kann die Geheimhaltung von Informationen zur Terrorismusbekämpfung die nationale Sicherheit erhöhen. In vielen Fällen ist die Aufrechterhaltung und das Bestehen von Informationsasymmetrien aber schädlich, weil dadurch beispielsweise Risikomanager und Entscheidungsträger nicht alle notwendigen Informationen zur Analyse und Bewertung eines Risikos erhalten und deswegen notwendige Bewältigungsmassnahmen vernachlässigen.
  Beispiel: Subprime-Krise USA (Investoren und Hausbesitzer bezüglich Risiken zu wenig informiert)

- ***Öffentliches Verständnis und Toleranz von Risiken:*** Neben der wissenschaftlichen und objektiven Analyse von Risiken werden grosse Risiken in der Gesellschaft immer auch von der breiten Öffentlichkeit bewertet, wobei diese Einschätzung von der objektiven Bewertung abweichen kann: Neben der Einschätzung der Eintrittswahrscheinlichkeit und der Höhe der Auswirkungen spielen für das öffentliche Verständnis und für die öffentliche Toleranz der Risiken folgende Faktoren eine wesentliche Rolle: kulturelle Werte, persönliche Kontrollierbarkeit des Risikos, Verteilung der Auswirkungen auf die Bevölkerung, Familiarität des Risikos, menschliches Verschulden des Risikos, bewusstes Tragen des Risikos durch die Bevölkerung usw. Um die Akzeptanz von Entscheiden im Umgang mit solchen Risiken zu erhöhen müssen solche Überlegungen im Risikomanagement mit einbezogen werden.
  Beispiel: Gentechnik (unterschiedliche Risikowahrnehmung in USA und EU), Problematik radioaktiver Abfall, Klimawandel, …

- ***Erkennen von und Handeln in unerwarteten Situationen***: Einerseits existieren bei der Identifikation von neuen Risiken häufig kognitive Barrieren. Das heisst viele Menschen haben Mühe, Ereignisse ausserhalb von akzeptierten Paradigmen zu erkennen. Um dem entgegenzuwirken ist es wichtig, bei der Identifikation von Risiken einen Fokus auf Kreativität zu legen und beispielsweise auch Querdenker in der Risikoidentifikation mit einzubeziehen. Andererseits kann manchmal eine Organisation auf schnelle Änderungen nicht situationsgerecht reagieren. In diesen Fällen ist eine Haltung und Kultur anzustreben, die Entscheidungen unter Unsicherheit und die Fähigkeit, von vorhandenen und nicht mehr geeigneten Abläufen und Strukturen Abschied zu nehmen, fördert.
  Beispiel: 9/11-Terroristenangriff auf Twin-Towers (unerwartete Angriffsmethode)

Anhang 10: Factsheets «Querschnittsrisiken Bund»

In diesem Anhang werden spezifische Querschnittsrisiken in der Bundesverwaltung analysiert und erläutert. Ein klares und gemeinsames Verständnis dieser Risiken sollen den bundesweiten Umgang mit diesen verbessern.

Die Ausführungen zu den einzelnen Risiken sind in diesen Kapiteln wie folgt strukturiert:

- *Risikoanalyse:* Terminologie, allfällige Unterteilung in Unterrisiken, Wechselwirkungen etc.;
- Involvierte *Akteure* und ihre Aufgaben im Risikomanagementprozess;
- *Zusammenarbeit* der Akteure;
- *Zentrale Kompetenzstellen* für das Querschnittsrisiko respektive das Querschnittsthema, weitere Informationen;
- *Massnahmenoptionen und Best Practices* im Umgang mit dem Querschnittsrisiko respektive Querschnittsthema;
- *Empfehlungen* der Koordinationsstelle Risikomanagement Bund.

Folgende Querschnittsrisiken werden in diesem Anhang analysiert:

A) IKT-Risiken

B) Infrastrukturrisiken (ohne IKT-Risiken)

C) Vermögensdelikte

D) Personalrisiken

E) Ungenügende Ordnungsmässigkeit der Staatsrechnung

A) IKT-Risiken

Risikoanalyse

Informations- und Kommunikationstechnologien (IKT) werde heute vielseitig eingesetzt. Sie unterstützen in den Departementen und VE die Geschäftsprozesse zur Erfüllung der Aufgaben. Alle Ereignisse und Entwicklungen im IKT-Umfeld, die negative Auswirkungen auf die Erfüllung der Aufgaben oder auf die Zielerreichung des Bundes haben, sind als IKT-Risiken der Bundesverwaltung zu betrachten. Für einen IKT-Leistungserbringer (LE) ist der Ausfall bzw. die Störung der IKT-Infrastruktur *an sich* ein Risiko, da der Betrieb der IKT-Systeme zugunsten ihrer Leistungsbezüger (LB) ihre Hauptaufgabe darstellt. Um den sichern Betrieb der IKT-Leistungen zu gewähren, ist der LE auf verlässliche Lieferanten angewiesen. IKT-Risiken treten häufig verwaltungseinheits- und departementsübergreifend auf, was ihre Bewirtschaftung komplex macht.

Grundsätzlich werden vier Arten von Beeinträchtigungen der IKT-Systeme unterschieden. Je nach konkretem Szenario können mehrere Beeinträchtigungen gleichzeitig auftreten. Alle unterbrechen oder stören wichtige Geschäftsprozesse und können zu finanziellen Folgen und Reputationsschäden führen:

a. Ausfall von Anwendungen oder/und Nichtverfügbarkeit von Daten (Verfügbarkeitsrisiko)
b. Abfluss von sensiblen Daten (Vertraulichkeitsrisiko)
c. Manipulation von Daten (Integritätsrisiko)
d. Daten können unbemerkt verändert werden (Nachvollziehbarkeit und Integrität)

Diese Beeinträchtigungen können die Folge sein von zahlreichen Ursachen, die ihrerseits als Risiken angesehen werden können. Nachfolgend eine nicht abschliessende Aufzählung solcher Risiken:

- Spionagetätigkeiten
- Cyberattacken
- Malware (Viren, Trojaner etc.)
- Elementarereignisse (Brand, Wasser etc.)
- Archivierungs- und Speicherungsprobleme
- Nicht-Kompatibilität von IT-Systemen
- ungenügende Leistungsfähigkeit von Systemen
- fehlendes IT-Know-How
- Fahrlässigkeit von Mitarbeitenden im Umgang mit Daten und Anwendungen
- IT-Insellösungen und Schnittstellenrisiken (insbes. auch bei Outsourcing von IKT-Dienstleistungen)
- zu weit gefasste Zugriffsberechtigungen
- alternde bzw. nicht mehr gewartete Technologien/Plattformen
- Projektverzögerungen bei Entwicklung von neuen IKT-Systemen
- Abhängigkeitsrisiken beim Einsatz von externen Leistungserbringern bzw. Beratern

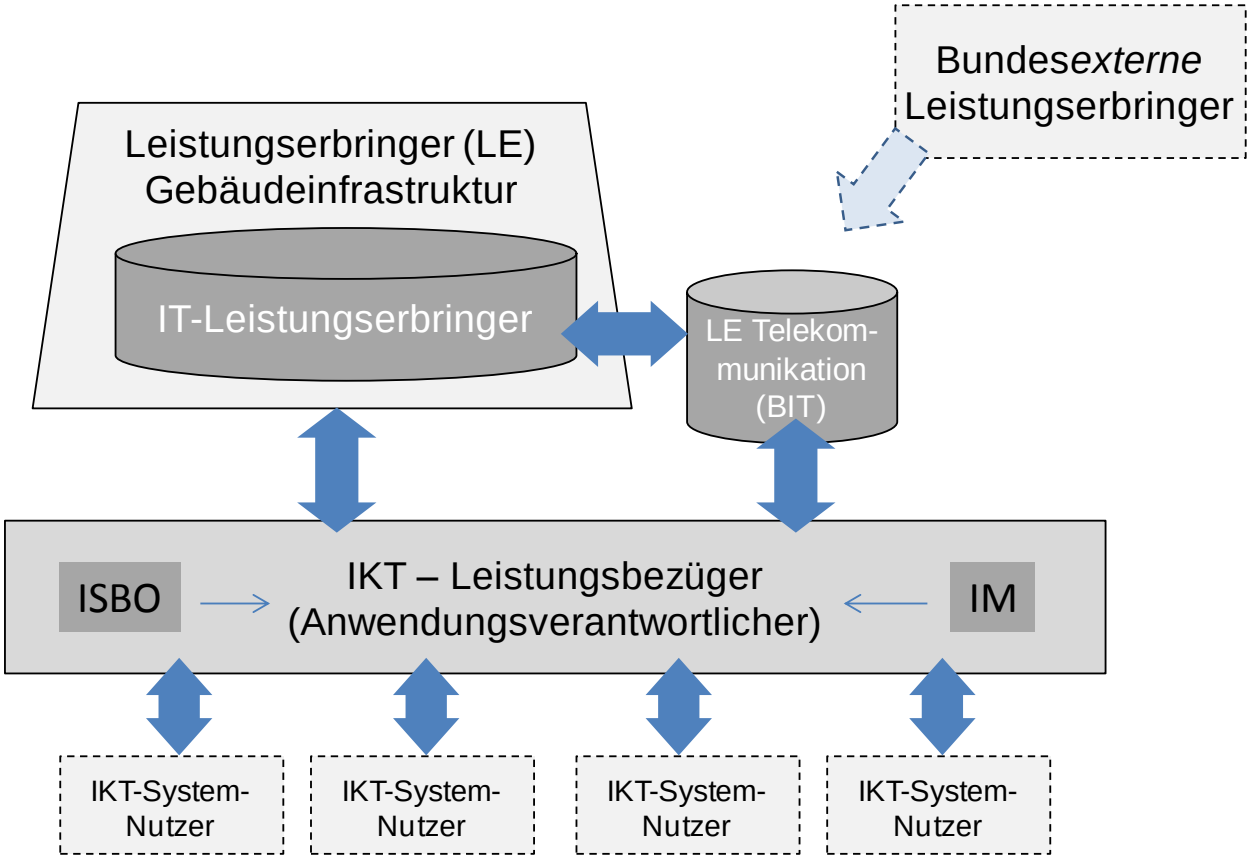
Normalerweise wird für jede IKT-Anwendung bzw. die darin enthaltenen Daten der erforderliche Schutzbedarf eruiert. Hierzu erstellt der Datenherr eine Schutzbedarfsanalyse. Besteht ein höherer Schutzbedarf der Daten, muss ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) erstellt werden. Darauf aufbauend wird i.d.R. zwischen dem IKT-LE und IKT-LB ein Service Level Agreement (SLA) abgeschlossen.

Beispiele von Wechselwirkungen mit IKT-Risiken:

▪ IKT-Infrastrukturrisiken am Standort (Brand, Überschwemmung, Stromausfall etc.) können zu Ausfällen von IKT-Systemen und Anwendungen beim LB führen.[93] ▪ Geeignete IKT-Massnahmen können ein Veruntreuungsrisiko reduzieren.	
Akteure und ihre Aufgaben im Risikomanagementprozess	
IKT-LE/Bereitsteller (BIT[94], FUB; ISC-EJPD, ISCeco, Informatik EDA, ZAS)	*Risikoidentifikation:* insb. Infrastrukturrisiken für den IKT-Betrieb; *Risikobewertung:* insb. Einschätzung der Eintrittswahrscheinlichkeit und der Auswirkungen auf der Bereitstellungsebene; *Risikobewältigung:* Massnahmenevaluation (zusammen mit dem LB) und Massnahmenumsetzung auf LE-Ebene; *Überwachung:* insb. der technischen Massnahmen und von Änderungen im technischen Umfeld.
IKT-LB/Anwender[95]	*Risikoidentifikation:* insb. auf personeller und organisatorischer Ebene; *Risikobewertung:* insb. die Auswirkungen auf die Aufgabenerfüllung bzw. die Geschäftsprozesse der VE; *Risikobewältigung:* Evaluation von und Entscheid über Massnahmen (inkl. Definition der Risikotoleranz bzw. der Sicherheitsanforderungen); Umsetzung der Massnahmen auf Anwenderseite; *Überwachung:* insb. auch der IKT-Nutzer
LE Gebäudeinfrastruktur für IKT (BBL, ar)	*Risikoidentifikation:* insb. in Bezug auf den Einfluss von Infrastrukturrisiken (z. B. Stromunterbrüche) auf IKT-Risiken; *Risikobewertung*: insb. die Auswirkungen auf die Aufgabenerfüllung der IKT-LE *Risikobewältigung:* Evaluation und Umsetzung von baulichen und gebäudetechnischen Massnahmen; *Überwachung:* insb. von baulichen und gebäudetechnischen Massnahmen.
IKT-Nutzer[96]	*Risikoidentifikation: –* *Risikobewertung: –* *Risikobewältigung:* Umsetzung von personellen und organisatorischen Massnahmen (Passwörter etc.); *Überwachung: –*
Bundesexterne LE (Swisscom, EWB, Software-Anbieter etc.)	Es ist wichtig, beim Abschluss von Verträgen mit bundesexternen LE auf ihren Einfluss auf die Systeme des Bundes und die damit verbundenen Risiken zu achten und diese wo möglich zu reduzieren (BCM mit Lieferanten abstimmen).

[93] In der Regel wird zwischen dem IKT-LE und dem BBL bzw. armasuisse die erforderliche Gebäudeinfrastruktur-Sicherheit in einem SLA festgelegt.
[94] Das BIT ist nicht nur Informationstechnik-LE für mehrere Departemente, es ist auch Hauptleistungserbringer im Bereich der bundesweiten Telekommunikation (Netze) und zudem bundesweit verantwortlich für die Generierung der digitalen Zertifikate (PKI = Public Key Infrastruktur).
[95] Beratend zum Thema IKT-Sicherheit bzw. IKT-Anwendungen stehen den LB/Anwendern in den Departementen und Ämtern die sog. Informatiksicherheitsbeauftragten (ISBD bzw. ISBO) und der Integrationsmanager (IM) zur Verfügung.
[96] IKT-Systemnutzer können auch bundesverwaltungsexterne Benutzer wie Firmen/Bevölkerung/ Kantone sein, die auf die IKT des Bundes zugreifen können. Diese sollen in das RM mit einbezogen werden (insb. wegen der Sicherheit).

Zusammenarbeit der Akteure



Zentrale Kompetenzstellen; weitere Informationen

Zentrale Kompetenzstellen:

- ***Informatiksteuerungsorgan Bund (ISB)***: Vorgeben und Überwachen der IKT-Strategie Bund; Beschliessen, Führen und Überwachen der Standarddienste IKT[97], Führen von E-Government und von MELANI.
- ***Melde- und Analysestelle Informationssicherung (MELANI)***: Vom Bundesrat mit dem Schutz kritischer Infrastrukturen[98] vor Gefahren aus dem Cyberspace beauftragt. Kompetenzstelle und Austauschplattform für Themen der IKT-Sicherheit, insb. Malware (Viren, Trojaner etc.) aus dem Internet. Innerhalb von MELANI ist *GovCERT.ch* angesiedelt, die Analysen von Schadsoftware durchführt und die Ergebnisse den Mitgliedern eines geschlossenen Kundenkreises zukommen lässt.[99]
- ***Bundesamt für Bauten und Logistik (BBL)***: Verantwortlich für die Unterbringung der zivilen Bundesverwaltung inkl. IKT-Infrastruktur.
- ***Armasuisse (ar)***: Verantwortlich für alle Immobilien des VBS inkl. IKT-Infrastruktur.

[97] Bspw. Büroautomation, Datenkommunikation.
[98] Als «Kritische Infrastrukturen» gelten Dienstleistungen, die bei einem mehrtägigen Ausfall weit greifende Konsequenzen für einen grossen Teil der Bevölkerung hätten.
[99] Während GovCERT.ch ausschliesslich für den zivilen Teil des Bundesnetzes sowie für die Betreiber kritischer Infrastrukturen zuständig ist, übernimmt MilCERT im militärischen Bereich gewisse CERT-Funktionen.

- ***Sonderstab Information Assurance (SONIA)****:* Krisenstab, der bei Krisen zusammentritt, die durch Störungen in der Informations- und Kommunikationsinfrastruktur ausgelöst werden. Hat gegenüber dem BR beratende Funktion und schlägt Massnahmen zur Bewältigung der Krise vor.

- ***Bundesamt für wirtschaftliche Landesversorgung (BWL)****:* Unter anderem strategische Beobachtung der IKT-Entwicklungen und Ergreifen entsprechender Massnahmen.[100]

Weitere Informationen und Unterlagen:

- ***IKT-Strategie des Bundes***
- ***Weisungen über die Informatiksicherheit in der Bundesverwaltung (WisB)***

Massnahmenoptionen und Best Practices

In einem umfassenden Konzept (i.d.R. ISDS-Konzept) sollen der benötigte Schutzbedarf festgehalten und die notwendigen Massnahmen definiert werden. Regelmässige Aktualisierungen (z. B. bei einem neuen Release der Anwendung) sind durchzuführen. Nachfolgend eine Aufzählung möglicher Massnahmen zur Reduktion von IKT-Risiken:

Organisatorische und personelle Massnahmen:

- Restriktive Zugriffsbeschränkungen für Anwendungen und Daten
- Restriktive Zugangsbeschränkungen zur IKT-Infrastruktur
- 4-Augen-Prinzip pflegen
- Sicherer Umgang mit und Verwendung von starken Passwörtern
- IT-Governance[101] (u. a. auch Nutzungsregeln für Internet und Software)
- Vorbereitung und Einübung eines Business Continuity-Plans für den Fall des Eintritts eines unvorhergesehenen Ereignisses

Technische Massnahmen:

- Einsetzen von Firewall und Antivirenprogramm
- Regelmässiges Back-Up von Daten
- Technische Aufzeichnung der Änderungen an Daten (Erhöhung der Nachvollziehbarkeit)
- Datenverschlüsselung
- Führen von IT-Ereignisprotokollen (sog. Log-Files; sie erhöhen die Nachvollziehbarkeit von Ereignissen)
- Einrichten von automatischen Kontrollen in den Systemen (Plausibilitätskontrolle)

Empfehlungen der EFV an Risikomanager und Risikocoaches

1. ***Prüfen, ob eine Aggregierung notwendig oder sinnvoll ist:***
   - Bei departements- oder verwaltungseinheitsübergreifenden Wechselwirkungen und Auswirkungen sollen IKT-Risiken i.d.R. aggregiert werden, vor allem wenn wichtige Geschäftsprozesse betroffen sind. Dies stellt sicher, dass die Wechselwirkungen verstanden, die Gesamtbedeutung erkannt und gemeinsame Massnahmen abgestimmt umgesetzt werden können. Die Koordinationsstelle empfiehlt, auf Stufe Leistungserbringer, Departement und/oder Bund eine Aggregation durchzuführen.
2. ***Prüfen, ob bereits eine zentrale Steuerung existiert:***
3. Auf Stufe Bund hat das ISB in diversen Bereichen eine Steuerungsfunktion bei den IKT-

[100] Vom Erdbeben und dem nachfolgenden Tsunami in Japan waren u. a. auch diverse Hersteller von Computerfestplatten betroffen, was weltweit zu Versorgungsengpässen führte. Das BWL trifft für Ereignisse dieser Art Vorsorgemassnahmen (z.B. Einrichten von Lagerbeständen).
[101] Vgl. ISACA, www.isaca.ch

Risiken. Wo das nicht der Fall ist, muss eine Aggregation unter Federführung der Risikocoaches der Leistungserbringer, der Risikomanager der Departemente und/oder der Koordinationsstelle Bund durchgeführt werden.***Informationen beschaffen und Aufgaben bzw. Verantwortlichkeiten klären:***

- Sicherstellen, dass alle betroffenen VE bzw. Abteilungen das zu aggregierte IKT-Risiko in ihrem Bereich analysiert und bewertet haben.
- Prüfen bzw. sicherstellen, dass Aufgaben, Verantwortlichkeiten, Schnittstellen etc. in Bezug auf die Risikobewirtschaftung geklärt sind, z. B. in Service Level Agreements (SLA).
- IKT-Risiken nötigenfalls in Teilrisiken aufsplitten, damit klare Verantwortlichkeiten zugeteilt werden können.

4. ***Reporting des aggregierten Risikos:***
   - Die betroffenen IKT-Anwendungen sind aufgrund der zu erwartenden Auswirkungen bei Eintritt des Risikos zu priorisieren. Daraus ergibt sich der «credible worst case» und auch die Priorisierung der Massnahmen.
   - Sicherstellen, dass Wechselwirkungen aufgezeigt werden und in die Analyse mit einbezogen wurden.
   - Zurückhaltung bei der Aggregation von zu unterschiedlichen IKT-Risiken[102].
5. ***Informationsaustausch:***
   - Die Zusammenarbeit zwischen den Informatiksicherheitsbeauftragten der Verwaltungseinheiten (ISBO's) und den Risikocoaches soll verbessert werden.
   - Einheitliches Vorgehen bei Analyse und Bewertung des zu aggregierenden IKT-Risikos sicherstellen. Nötigenfalls Workshops mit allen Beteiligten. Koordination von Massnahmen unterstützen.
   - Informationsaustausch allgemein fördern (insb. zwischen LE und LB).

[102] Eine Aggregation «IKT-Risiken» ist z. B. kaum sinnvoll.

B) Infrastrukturrisiken (ohne IKT-Risiken)

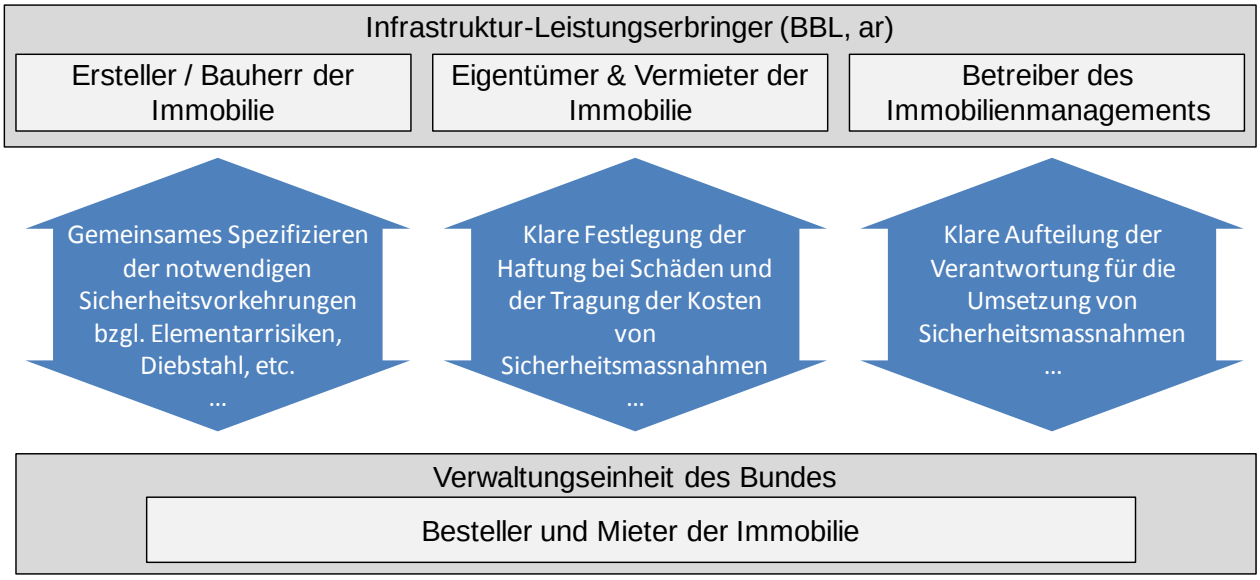
Risikoanalyse
Unter Infrastrukturrisiken werden alle Risiken verstanden, die negative Auswirkungen auf die Infrastruktur in der Bundesverwaltung haben. Unter Infrastruktur sind in erster Linie alle Immobilien der Bundesverwaltung inkl. der für deren Betrieb notwendigen Infrastruktur zu verstehen. Explizit ausgeschlossen sind hier die Informations- und Kommunikationstechnologien[103], die häufig durch andere OE betrieben werden. (vgl. Kapitel 3). Bei Fragen der Gebäude- und Personen*sicherheit* ist zudem auch der Bundessicherheitsdienst mit einbezogen. Folgende Ereignisse (nicht abschliessend) können unter den Begriff «Infrastrukturrisiken» subsummiert werden: a. Elementarereignisse (Hochwasser, Erdbeben, Lawinen) b. Brand c. Stromunterbrüche d. Einbruch und Diebstahl e. Unbefugter Zugang (z.B. in Rechenzentren etc.) f. Vandalismus Bei all diesen Risiken können grössere Sachschäden zu finanziellen Auswirkungen führen. Neben den Sachschäden sind in diesem Zusammenhang v.a. auch die Unterbrüche in den Tätigkeiten und Prozessen der VE zu berücksichtigen und zu bewerten. Es können auch Verletzte und Tote und (je nach Verschulden) auch Reputationsschäden entstehen. Aufgrund der geografischen Unterschiede und der unterschiedlichen Nutzung muss für *jede Immobilie* eine individuelle Analyse der verschiedenen Infrastrukturrisiken durchgeführt werden. Schon beim Bau einer neuen Immobilie können erste Massnahmen zum Schutz gegen Infrastrukturrisiken geplant und umgesetzt werden. Dies bedingt in der Bauphase (schon ab Projektbeginn) eine gute Zusammenarbeit zwischen dem Ersteller/Bauherr und dem späteren Nutzer des Gebäudes. Später muss in der Immobilienbewirtschaftung klar geregelt sein, wer welche Risiken trägt und wer welche sicherheitstechnischen Massnahmen umsetzt. Beispiele von Wechselwirkungen mit Infrastruktur-Risiken: ▪ der Eintritt eines grösseren Infrastrukturschadens (insb. Stromunterbruch) löst in der Regel auch ein IKT-Risiko aus, wenn wichtige IKT-Infrastruktur der Bundesverwaltung im betroffenen Gebäude untergebracht ist.
Akteure und ihre Aufgaben im Risikomanagementprozess

Infrastruktur-Bereitsteller (BBL, ar)	*Risikoidentifikation*: insb. der bau- und gebäudetechnischen Risiken *Risikobewertung*: insb. Eintrittswahrscheinlichkeiten von technischen Risiken (Brand, etc.) *Risikobewältigung*: Vorschläge für technische Massnahmen erarbeiten und Massnahmen umsetzen *Überwachung*: der baulichen (und z.T. organisatorischen) Massnahmen.

[103] Ausser die WLAN-Anlagen, welche durch den Gebäudeinfrastruktur-Leistungserbringer bereitgestellt werden.

Verwaltungseinheit als Mieter	*Risikoidentifikation* *Risikobewertung:* insb. Auswirkungen auf die Geschäftsprozesse der VE *Risikobewältigung*: Vorschläge für Massnahmen erarbeiten und Umsetzung bzgl. der Gebäude- und Personensicherheit. *Überwachung*: v.a. der organisatorischen Massnahmen.

Zusammenarbeit der Akteure


Infrastruktur-Leistungserbringer (BBL, ar)
Ersteller / Bauherr der Immobilie
Eigentümer & Vermieter der Immobilie
Betreiber des Immobilienmanagements
Gemeinsames Spezifizieren der notwendigen Sicherheitsvorkehrungen bzgl. Elementarrisiken, Diebstahl, etc.
...
Klare Festlegung der Haftung bei Schäden und der Tragung der Kosten von Sicherheitsmassnahmen
...
Klare Aufteilung der Verantwortung für die Umsetzung von Sicherheitsmassnahmen
...
Verwaltungseinheit des Bundes
Besteller und Mieter der Immobilie

Zentrale Kompetenzstelle und weitere Informationen

Bundesamts für Bauten und Logistik (BBL): Wichtige Informationen zu den Dienstleistungen (z.B. Kontroll- und Sicherheitsdienstleistungen) des BBL finden sich auf der bundesinternen BBL-Kundenplattform.

Massnahmenoptionen und Best Practices

- Definition von Rettungsausgängen und –wegen
- Vordefinierte Schliesspläne für Immobilie (Gebäudesicherung)
- Installation von Alarmanlagen (inkl. Videoüberwachung)
- Vorbereitung von Notfallprozessen/abläufen, Evakuierungsübungen[104]
- Gebäudezugangskontrollen
- Notfallorganisation vorbereiten
- Feuerlöscher & Sprinkleranlagen
- Gebäudesicherungssysteme
- Versicherungen abschliessen (bspw. Sachschäden)[105]

[104] Diese Massnahmen werden durch den Mieter/Nutzer umgesetzt.
[105] Aufgrund des Grundsatzes der Eigenversicherung werden in der Regel keine solche Versicherungen abgeschlossen. Die EFV ist für das Versicherungswesen zuständig.

Empfehlungen EFV an Risikomanager und Risikocoaches

1. ***Prüfen, ob eine Aggregation notwendig oder sinnvoll ist:***
   - Bei departements- oder verwaltungseinheitsübergreifenden Wechselwirkungen sollten Infrastruktur-Risiken i.d.R. aggregiert werden. Aufgrund der geografischen Nähe vieler Immobilien im Grossraum Bern empfiehlt die Koordinationsstelle, insb. die Risiken Stromunterbrüche[106] und Elementarereignisse aggregiert zu betrachten.
2. ***Prüfen, ob bereits eine zentrale Steuerung existiert:***
   - Die zentrale Steuerung der Infrastrukturen des Bundes erfolgt auf Stufe der Leistungserbringer (BBL, ar). Eine Aggregation der Risiken vorerst auf Stufe der Leistungserbringer, BBL und ar sollte umgesetzt werden.
3. ***Informationen beschaffen und Aufgaben bzw. Verantwortlichkeiten klären:***
   - Sicherstellen, dass alle betroffenen VE bzw. Abteilungen das zu aggregierende Infrastruktur-Risiko in ihrem Bereich analysiert und bewertet haben.
   - Prüfen bzw. sicherstellen, dass Aufgaben, Verantwortlichkeiten, Schnittstellen etc. in Bezug auf die Risikobewirtschaftung geklärt sind, z.B. in Service Level Agreements (SLA).
4. ***Reporting des aggregierten Risikos:***
   - Die betroffenen Geschäftsprozesse sind aufgrund der Einschätzung der zu erwartenden Auswirkungen bei Eintritt des Risikos zu priorisieren. Daraus ergibt sich der «credible worst case» und auch die Priorisierung der Massnahmen.
5. ***Informationsaustausch:***
   - Informationsaustausch zwischen den Leistungserbringern und zwischen Leistungserbringer und den Verwaltungseinheiten als Nutzer fördern.

[106] Für längerfristige Unterbrüche existiert eine interdepartementale Arbeitsgruppe „Priorisierung der Bundesgebäude bei Strommangellagen“.

C) Vermögensdelikte

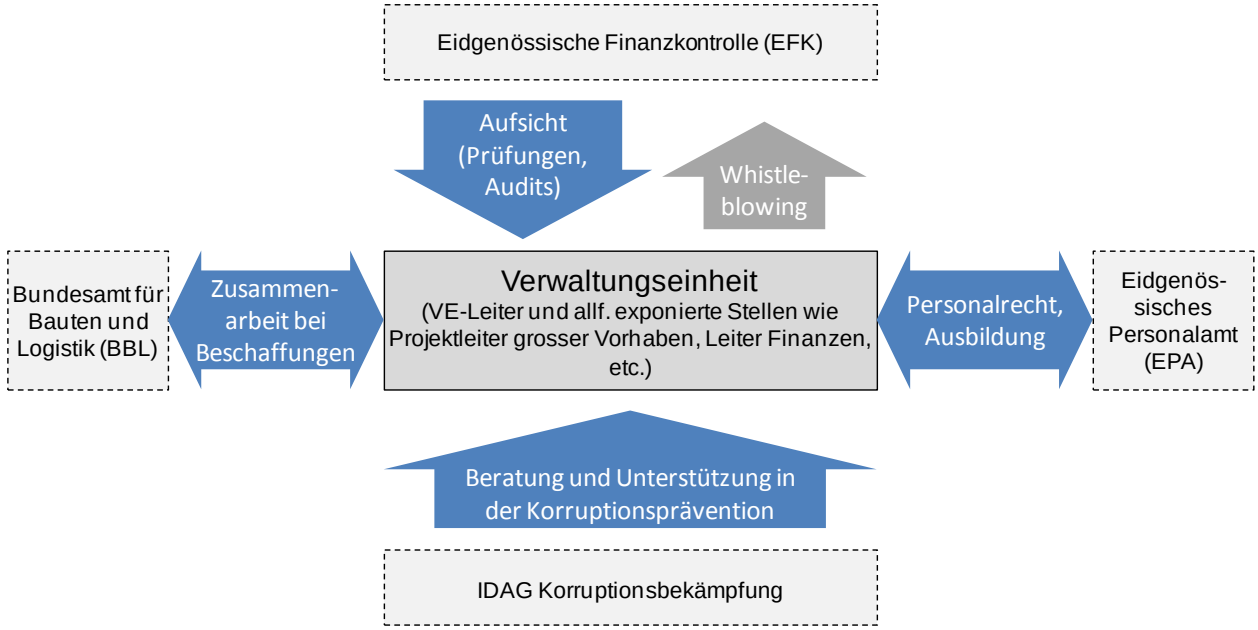
Risikoanalyse
Unter ***Korruption*** wird der Missbrauch einer Vertrauensstellung zur Erlangung eines ungerechtfertigten materiellen oder immateriellen Vorteils verstanden. Konkrete Fälle von Korruption sind bspw. Bestechung, Vorteilsannahme und Vorteilsgewährung. Bei der ***Veruntreuung*** geht es um die unberechtigte Aneignung von Vermögenswerten durch Mitarbeitende der Bundesverwaltung. Bei der ***ungetreuen Amtsführung*** werden bei einem Rechtsgeschäft die von den Angestellten zu wahrenden öffentlichen Interessen geschädigt, um sich oder einem andern einen unrechtmässigen Vorteil zu verschaffen. Bei ***Insidergeschäften*** werden nicht-öffentliche Informationen von einem Mitarbeitenden zur eigenen Bereicherung ausgenutzt. Neben den finanziellen Auswirkungen solcher Risiken, zum Beispiel durch die Bezahlung überhöhter Preise im Beschaffungswesen, ist insbesondere das Risiko für Reputationsschäden beträchtlich. Nicht alle Verwaltungseinheiten sind von Korruption und Veruntreuung gleich stark betroffen. Besonders korruptionsanfällig sind zum Beispiel die Vergabe öffentlicher Aufträge oder Kontakte mit Staaten, die in internationalen Korruptionsratings schlecht abschneiden, aber auch die Steuer-, Revisions-, Aufsichts- und Konzessionserteilungsbereiche, der Grenzkontrollsektor und die Bereiche Justiz und Polizei. Ungetreue Geschäftsführung kann vermehrt in Bereichen eintreten, in denen Finanzflüsse und Zahlungen gesteuert und ausgelöst werden. Die Haupt*ursache* für diese Risiken ist der Mensch und sein Umfeld. Ein Nährboden für diese Risiken bildet bspw. eine unzureichende Bindung oder Loyalität des Arbeitsnehmers ggü. dem Arbeitgeber oder eine erhöhte Anonymität in der Organisation. Weiter können auch Arbeitsplatzunzufriedenheit, Frustration, fehlende Motivation oder ungenügende Kontrollen bzw. eine ungenügend klare, geordnete Organisation der Abläufe und Prozesse zu Korruptions- und Veruntreuungshandlungen verleiten. *Wechselwirkungen*: ▪ Aufgedeckte Fälle von Korruption und Veruntreuung können zur Entlassung der involvierten Personen führen; dies kann zu einem „Know-How"-Verlust und zur Verunsicherung des Personals führen sowie weitere Mängel in den Organisationsabläufen aufdecken.

Akteure und ihre Aufgaben im Risikomanagementprozess	
Verwaltungseinheit (insb. Leiter VE; aber auch Grossprojekt-Leiter, Leiter Finanzen, Compliance&Risk Abteilungen etc.)	*Risikoidentifikation*: ja, insb. Identifizieren von sensiblen Arbeitsstellen innerhalb seines Bereiches *Risikobewertung*: ja *Risikobewältigung*: ja, verantwortlich für die Definition und Umsetzung von Massnahmen. *Überwachung*: ja
Eidgenössische Finanzkontrolle (EFK)[107]	*Risikoidentifikation*: ja, im Rahmen der Rolle als Whistleblowing Stelle des Bundes. *Risikobewertung*: ja *Risikobewältigung*: Empfehlungen zur Reduktion von Korruptions- und Veruntreuungsrisiken

[107] Vgl. http://www.efk.admin.ch/index.php?option=com_content&view=article&id=223&Itemid=238&lang=de

	Überwachung: Audits/Revisionen[108]
IDAG Korruptionsbekämpfung (Federführung EDA)	*Risikoidentifikation:* - *Risikobewertung:* - *Risikobewältigung*: insb. Vorschläge für Massnahme-*Strategien* erarbeiten.[109] *Überwachung*: ja, IDAG Kerngruppe
Bundesamt für Bauten und Logistik (BBL)[110]	*Risikoidentifikation*: im Bereich Beschaffung *Risikobewertung*: - *Risikobewältigung*: setzt Massnahmen zur Reduktion des Korruptionsrisikos in der Beschaffung um. *Überwachung*: -
Eidgenössisches Personalamt (EPA)	*Risikoidentifikation*:- *Risikobewertung*:- *Risikobewältigung*: ja, bundesweite Massnahmen (Vorschriften, Ausbildung, etc.) *Überwachung*: -

Zusammenarbeit der Akteure[111]



Zentrale Kompetenzstellen und weitere Informationen

Für Korruption:

- Die ***Interdepartementale Arbeitsgruppe (IDAG) zur Korruptionsbekämpfung*** erarbeitet Strategien zur Korruptionsbekämpfung auf nationaler und internationaler Ebene und lanciert Sensibilisierungs- und Informationskampagnen:

[108] Die EFK führt Audits nicht nur im Bereich Korruption durch, sondern in vielen unterschiedlichen Bereichen wie z.B. IT-Sicherheit, IKS etc.
[109] Vgl. Bericht an den Bundesrat März 2011 und Massnahmen für Prävention von Korruption
[110] Analog hat die armasuisse diese Funktion für die militärische Beschaffung.
[111] Das EPA informiert im Rahmen von Personalrechtsausbildungen über die allgemeinen Verhaltensregeln (Verhaltenskodex) der Angestellten und Vorgesetzten. Über die departements- bzw. amtsspezifischen Weisungen nach Art. 94*d* BPV informieren die Departemente und Ämter intern selber.

- Das ***Bundesamt für Bauten und Logisitik*** (BBL) ist für das Beschaffungswesen des Bundes zuständig und hat Erfahrung im Bereich der Korruptionsprävention.[112] Es bietet neben Beratungen in der Beschaffung auf seiner Website u.a. ein Faktenblatt zum Thema Korruptionsprävention und Beratung an.

Weitere Informationen:

- ***GIMAP***: Beschaffungswegweiser und interaktiver Führer zum Thema öffentliches Beschaffungswesen
- ***Bundespersonalgesetz*** und ***Bundespersonalverordnung*** enthalten Verhaltensvorschriften für Mitarbeitende (bspw. Art 20, 21 Abs. 3 und 23 BPG, Art. 91 bis 94*d* BPV).
- Weitere Ausführungen finden sich im ***Verhaltenskodex Bundesverwaltung***[113] sowie in den ***Richtlinien zu Nebenbeschäftigungen und öffentlichen Ämtern*** *(EPA)*[114]
- Broschüre Korruptionsprävention und Whistleblowing[115]

Massnahmenoptionen und Best Practices

- Einrichtung und Bekanntmachung der Whistleblowing-Stelle[116] bei der EFK
- Verhaltenskodex Bundesverwaltung und Verhaltensweisungen der Departemente und Ämter gestützt auf Art. 94*d* BPV (Ausstandsregeln, Annahme von Geschenken, etc.)[117]
- Regelmässige Information, Sensibilisierungsmassnahmen (insb. durch IDAG Korruptionsbekämpfung) und Schulung der Mitarbeitenden[118]
- Audits und Stichproben
- interne Kontrollen, bspw. das Vier-Augen-Prinzip[119] (hier ist nicht nur die formelle sondern auch die materielle Prüfung wichtig)
- systemtechnische Kontrollen und Massnahmen (z.B. Zugriffsbeschränkungen und Freigabeerfordernisse, elektronische Visierung)
- materielle Überprüfung der Waren und Dienstleistungen (bei grösseren Zahlungen).
- Konsequente Funktionstrennungen
- Personensicherheitsüberprüfungen bei exponierten Stellen
- Einholen von Referenzen und Prüfung von amtlichen Registern bei Neuanstellungen
- Vorbildfunktion der Vorgesetzten
- Loyalität der Mitarbeitenden erhöhen
- Einführung der Meldepflicht für Mitarbeitende (Artikel 22a im BPG)

Spezifische Massnahmen zur Verminderung von Korruption:

- Unbefangenheitserklärungen von exponierten Personen
- Verpflichtung zu schriftlichen Verträgen in der Beschaffung
- Zentrales und transparentes Beschaffungsverfahren[120]
- Integritätsklausel in Verträgen mit Lieferanten
- Begründung und Dokumentation von Verfahren und Vergabeentscheiden

---

[112] Beim BBL sind auch die Beschaffungskommission des Bundes (BKB) und das Kompetenzzentrum Beschaffungswesen Bund (KBB) angegliedert.
[113] BBl 2012 7873
[114] In diversen VE wurden spezifischere Verhaltensweisungen erarbeitet (bspw. EFV).
[115] Vgl. http://www.epa.admin.ch/dokumentation/publikationen/index.html?lang=de und http://www.admin.ch/ch/d/sr/c172_220_1.html
[116] Vgl. http://www.efk.admin.ch/index.php?option=com_content&view=article&id=223&Itemid=238&lang=de
[117] vgl. http://www.epa.admin.ch/dokumentation/publikationen/index.html?lang=de und http://www.admin.ch/ch/d/sr/c172_220_1.html
[118] Über Themen der Integrität, bspw. über Anzeigepflichten und Melderecht nach BPG.
[119] Dieses besagt, dass wichtige Entscheidungen nicht von einer einzelnen Person getroffen oder kritische Tätigkeiten nicht von einer einzelnen Person durchgeführt werden sollen oder dürfen, um das Risiko von Fehlern oder Missbräuchen zu reduzieren.
[120] Das Beschaffungsverfahren ist im Bundesgesetz über öffentliche Beschaffungswesen (BöB) und in der entsprechenden Verordnung geregelt (VöB).

- Risikobeurteilung bei der Vergabe von Aufträgen
- Konsequente Durchsetzung der Ausstandsregeln

Empfehlungen EFV an die Risikomanager bzw. Risikocoaches

1. ***Prüfen, ob eine Aggregation notwendig oder sinnvoll ist*:**
   - Da bereits diverse zentral umgesetzte Massnahmen bestehen (EPA, EFK, BBL etc.) und keine verwaltungseinheits- oder departementsübergreifenden Wechselwirkungen bestehen, würde eine Aggregation im Wesentlichen nur die Gesamtbedeutung des Querschnittsthemas aufzeigen. Die Verantwortung für die Bewirtschaftung dieser Risiken liegt bei den VE. Die Koordinationsstelle EFV empfiehlt vorerst keine Aggregation dieses Risikos.
2. ***Prüfen, ob zentrale Steuerung existiert*:**
   - Es existieren diverse zentrale Kompetenzstellen (siehe oben). Diese haben eine beratende Funktion, erarbeiten aber keine aggregierte Risikobetrachtung.

D) Personalrisiken

Risikoanalyse
Jede Verwaltungseinheit im Bund besteht aus und funktioniert nur mit fähigen Mitarbeitenden. Diese besitzen oder erwerben im Verlauf ihrer Tätigkeit Wissen bzw. ***Know-How***, das für das Funktionieren der VE wichtig bis existenznotwendig ist. Ein ***Ausfall*** solcher Personen, sei es auf Grund von Krankheit oder Unfall oder auf Grund einer Kündigung, kann zu Störungen im normalen Geschäftsverlauf der VE und zu Unterbrüchen in wichtigen Prozessen führen. Zudem kann der entstehende Know-How-Verlust zu (schwer quantifizierbaren) Mehrkosten führen (Rekrutierung, Einarbeitung, ineffiziente Erledigung der Aufgaben, etc.), was sich schlussendlich auch finanziell auswirkt. Ein ***Know-How-Mangel*** im Sinne von zu wenig qualifiziertem Personal entsteht in der Regel schleichend, wenn mittelfristig die Rahmenbedingungen für das Personal nicht attraktiv gestaltet werden bzw. die Weiterbildung der Mitarbeitenden nicht genügend ist. Externe Ursachen (z.B. keine geeignete Kandidaten mit entsprechenden Fähigkeiten in der Rekrutierungsphase) können das Problem zusätzlich verstärken. Unterschiedliche Ursachen können dazu führen, dass ein Know-How-Verlust oder ein Mangel an qualifiziertem Personal entsteht: Fehlende Motivation bestehender Mitarbeitenden (bspw. aufgrund von ungenügender Führung oder schlechter Kommunikation), Konzentration von Spezialwissen auf nur eine bzw. zu wenige Personen, fehlende Dokumentation von wichtigen Prozessen & Know-How, übermässiger Einsatz von externen Berater, etc. Die Geschwindigkeit, mit der ein Know-How-Ausfall eintritt (sehr schnell bei Todesfall vs. 3 Monate bei Kündigung vs. längerer Übergang bei Pensionierung) entscheidet massgeblich darüber, wie hoch die negativen Auswirkungen für die VE ausfallen. *Wechselwirkungen*: ▪ Ein Verlust eines Mitarbeitenden (MA) kann zu Schwierigkeiten in der Arbeitsbewältigung der verbliebenen MA bedeuten und in einem negativen Szenario mittelfristig weitere Abgänge nach sich ziehen.

Akteure und ihre Aufgaben im Risikomanagementprozess	
Mitarbeitender in einer Verwaltungseinheit	*Risikoidentifikation*: Erkennen von Prozessen und Know-How, wo eine Stellvertretung bzw. die Dokumentation des Know-Hows bzw. der Prozesse notwendig oder sinnvoll ist.[121] *Risikobewertung*: - *Risikobewältigung*: Evaluation von möglichen Massnahmen zusammen mit dem Vorgesetzten und Umsetzung von Massnahmen *Überwachung*: -
Führung/Vorgesetzter des Mitarbeitenden	*Risikoidentifikation*: Erkennen von Prozessen und Know-How, wo eine Stellvertretung bzw. die Dokumentation des Know-Hows bzw. der Prozesse notwendig oder sinnvoll ist.

[121] Dabei muss berücksichtigt werden, dass der einzelne Mitarbeitende einen tiefen Anreiz hat, sein Know-How (das einen Teil seiner Qualifikation und seines Marktwertes ausmacht) zu teilen oder zu dokumentieren. Aus diesem Grund hat die Führung und auch der Personalverantwortliche der Organisation umso mehr die Verantwortung für die Bewirtschaftung dieses Risikos.

	Risikobewertung: ja, Auswirkung eines Ausfalls eines/mehrerer Mitarbeitenden auf die Abteilung/Organisation einstufen. *Risikobewältigung*: Evaluation von möglichen Massnahmen (zusammen mit den Mitarbeitenden) und Massnahmenentscheide treffen (inkl. Definition der Risikotoleranz) *Überwachung*: ja
Personalverantwortlicher der Verwaltungseinheit	*Risikoidentifikation*: Mängel im Bereich Rekrutierung und Führung in der VE erkennen. *Risikobewertung*: - *Risikobewältigung*: Evaluation von möglichen VE-weiten Massnahmen und deren Umsetzung *Überwachung*: der Wirkung dieser Massnahmen.
Eidgenössisches Personalamt (EPA), inkl. HRK[122]	*Risikoidentifikation*: für bundesweite Risiken im Bereich Mitarbeiterrekrutierung und -bindung. *Risikobewertung*: - *Risikobewältigung*: Evaluation von möglichen bundesweiten Massnahmen und deren Umsetzung *Überwachung*: -

Zusammenarbeit der Akteure

Eidgenössisches Personalamt (EPA)
HRK
Ausbildungen, Grundlagen & Konzepte
Personalverantwortlicher der Verwaltungseinheit
Arbeitet mit den Führungskräften der VE zusammen, um gute Rahmenbedingungen im Personalbereich zu schaffen.
Vorgesetzte bzw. Leiter der Organisationseinheit
Zusammenarbeit mit dem Ziel, die Kontinuität der Arbeit der Mitarbeitenden auch bei ihrem Ausfall sicherzustellen.
Mitarbeitender
Mitarbeitender
Mitarbeitender
Mitarbeitender

HRK = Human Resources Konferenz

Zentrale Kompetenzstelle und weitere Informationen

Eidgenössisches Personalamt (EPA): Erarbeitet bundesweite Grundlagen und Konzepte (bspw. zum Thema Mitarbeiterbindung), integriert das Thema Know-How-Verluste in diverse (Kader-)Schulungen, etc.

- Grundlagendokumente: Personalstrategie Bundesverwaltung,

[122] Human Resources Konferenz; hat den Lead bei der Koordination und Umsetzung der bundesrätlichen Personalpolitik. Mitglieder sind die Personalchefs der Departemente und der Bundeskanzlei.

Massnahmenoptionen und Best Practices

- Stellvertretungen für die wichtigsten Funktionen/Stellen (durch Identifikation der wichtigsten Funktionen/Stellen bzw. Wissensträger)
- Aufbau eines Wissensmanagements, damit das Know-How nicht *nur* durch einzelne Personen getragen wird.
- Personalmarketing für die Rekrutierung von qualifiziertem Personal (zentral im EPA)
- Massnahmen zur Erhöhung der Mitarbeiterbindung (Retention Management): modernes Arbeitsumfeld, konkurrenzfähige Anstellungsbedingungen, Karriereentwicklungsmodelle, Kompetenzmodelle, etc. (zentral im EPA)
- Nachvollziehbare Dokumentation von Geschäftsprozessen
- Förderung des informellen Austausches zwischen Mitarbeitenden
- Zurückhaltung bei längerfristigem Einsatz von externen Berater
- Frühzeitige Nachfolgeplanung im Hinsicht auf Pensionierungen

Empfehlungen EFV

1. ***Prüfen, ob eine Aggregation notwendig oder sinnvoll ist:***
   - Aufgrund von bereits vorhandenen zentral umgesetzten Massnahmen (EPA; HRK) und aufgrund fehlender Wechselwirkungen zwischen den VE würde eine Risikoaggregation v.a. dem Zweck dienen, die Gesamtbedeutung des Querschnittthemas auf Stufe Departement und Bund aufzuzeigen. Die Verantwortung für die Bewirtschaftung dieser Risiken liegt bei den VE. Die Koordinationsstelle EFV empfiehlt vorerst keine Aggregation dieses Risikos.
2. ***Prüfen, ob bereits eine zentrale Steuerung existiert:*** Es existiert eine zentrale Kompetenzstelle (EPA). Diese hat eine rein beratende Funktion und führt keine Risikoaggregation durch.
3. ***Informationsaustausch:*** Ein regelmässiger Austausch zwischen den Personalverantwortlichen der unterschiedlichen VE kann hilfreich sein, um Ansätze und Ideen zur Minderung dieser Risiken auszutauschen und von guten Beispielen innerhalb der Bundesverwaltung zu lernen.

E) Ungenügendes IKS zur Sicherstellung der Ordnungsmässigkeit der Staatsrechnung

Risikoanalyse

Die Buchführung der Bundesverwaltung ist dezentral organisiert. Jede Verwaltungseinheit erfasst die Buchungsvorgänge selber und ist demnach auch selber für die Einhaltung der rechtlichen Vorschriften zur Ordnungsmässigkeit der Staatsrechnung verantwortlich. Die Finanzberichterstattung (Erstellung der Staatsrechnung) hingegen wird zentral in der Eidg. Finanzverwaltung vorgenommen.

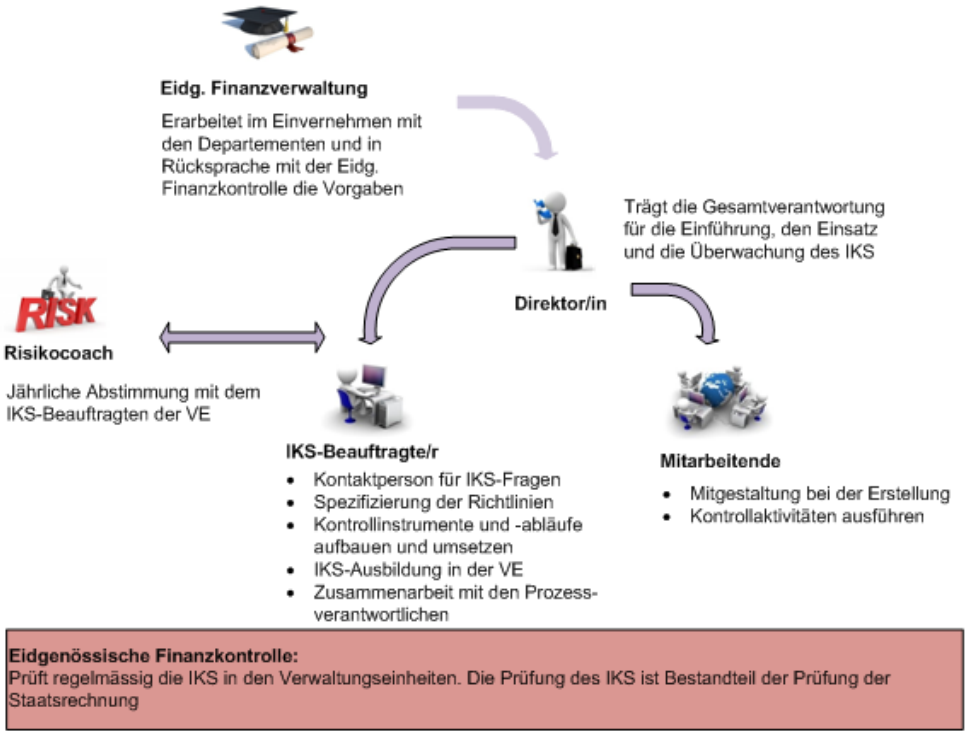
Die Ordnungsmässigkeit der Staatsrechnung umfasst folgende Aspekte:

- Grundsätze ordnungsmässiger Buchführung (Art. 38 FHG und 28 FHV):
  - Vollständigkeit: Alle Finanzvorfälle und Buchungstatbestände sind lückenlos und periodengerecht zu erfassen.
  - Richtigkeit: Die Buchungen müssen den Tatsachen entsprechen und sind nach den Weisungen der Eidg. Finanzverwaltung vorzunehmen.
  - Rechtzeitigkeit: Die Buchhaltung ist aktuell zu halten und der Geldverkehr tagesaktuell zu erfassen. Die Vorgänge sind chronologisch festzuhalten.
  - Nachprüfbarkeit: Die Vorgänge sind klar und verständlich zu erfassen. Korrekturen sind zu kennzeichnen und Buchungen durch Belege nachzuweisen.
- Grundsätze ordnungsmässiger Rechnungslegung (Art. 47 FHG und 54 FHV):
  - Wesentlichkeit: Es sind sämtliche Informationen offen zu legen, die für eine rasche und umfassende Beurteilung der Vermögens-, Finanz- und Ertragslage notwendig sind.
  - Verständlichkeit: Die Informationen müssen klar und nachvollziehbar sein.
  - Stetigkeit: Die Grundsätze der Budgetierung, Buchführung und Rechnungslegung sollen soweit als möglich über einen längeren Zeitraum unverändert bleiben.
  - Bruttodarstellung: Aufwände und Erträge sowie Investitionsausgaben und -einnahmen sind getrennt voneinander ohne gegenseitige Verrechnung in voller Höhe auszuweisen.

Das Interne Kontrollsystem (IKS) ist ein zentrales und geeignetes Instrument zur Sicherstellung der Ordnungsmässigkeit der Buchführung und Rechnungslegung in den Verwaltungseinheiten. Fehlt ein solches oder ist es in wesentlichen Teilen mangelhaft, besteht das Risiko, dass die veröffentlichte Finanzberichterstattung der Bundesverwaltung wesentliche Fehlaussagen enthält. Die Finanzberichterstattung des Bundes dient der öffentlichen Rechenschaftsablage gegenüber den Bürgern und als Entscheidungsgrundlage für Politiker, Anleger und Rating-Agenturen. Wesentliche Fehlaussagen in der Finanzberichterstattung ziehen deshalb nicht nur einen Reputationsschaden nach sich, sondern können auch die Entscheidungsgrundlagen für Politiker, Anleger und Rating-Agenturen verfälschen.

Akteure und ihre Aufgaben im Risikomanagementprozess	
Oberste Führungsebene (Direktorin / Direktor)	*Risikoidentifikation*: ja *Risikobewertung*: ja *Risikobewältigung*: ja, verantwortlich für das IKS in ihrem / seinem Zuständigkeitsbereich *Überwachung*: ja
IKS-Beauftragte/r	*Risikoidentifikation:* ja *Risikobewertung*: ja, die Risiko-Kontroll-Matrizes werden regelmässig überprüft und erneuert. *Risikobewältigung*: nein, höchstens für ihren / seinen Zuständigkeitsbereich als Linienvorgesetzte/r *Überwachung*: ja, koordiniert die Überwachungstätigkeiten in der VE
Prozessverantwortliche/r finanzrelevanter Geschäftsprozesse	*Risikoidentifikation:* ja, in ihrer / seiner Funktion als Linienvorgesetzte/r kennt die/der Prozessverantwortliche/r die Risiken in ihrem / seinem Prozess. *Risikobewertung*: ja, die Risiko-Kontroll-Matrizes werden regelmässig überprüft und erneuert. *Risikobewältigung*: ja, mittels Durchsetzung der IKS-Massnahmen in ihrem / seinem Zuständigkeitsbereich als Linienvorgesetzte/r *Überwachung*: ja, überwacht das Risikomanagement in ihrem / seinem Zuständigkeitsbereich.
Mitarbeitende in finanzrelevanten Geschäftsprozessen	*Risikoidentifikation*: nein *Risikobewertung*: nein *Risikobewältigung*: ja, bei der Durchführung der Kontrollen in der täglichen Arbeit. *Überwachung*: nein
Eidgenössische Finanzverwaltung	*Risikoidentifikation:* nein Risikobewertung: nein Risikobewältigung: nein Überwachung: nein
Eidgenössische Finanzkontrolle	*Risikoidentifikation:* ja *Risikobewertung*: ja *Risikobewältigung*: nein *Überwachung*: nein

Zusammenarbeit der Akteure


Eidg. Finanzverwaltung
Erarbeitet im Einvernehmen mit den Departementen und in Rücksprache mit der Eidg. Finanzkontrolle die Vorgaben
Trägt die Gesamtverantwortung für die Einführung, den Einsatz und die Überwachung des IKS
Direktor/in
RISK
Risikocoach
Jährliche Abstimmung mit dem IKS-Beauftragten der VE
IKS-Beauftragte/r
• Kontaktperson für IKS-Fragen
• Spezifizierung der Richtlinien
• Kontrollinstrumente und -abläufe aufbauen und umsetzen
• IKS-Ausbildung in der VE
• Zusammenarbeit mit den Prozess-verantwortlichen
Mitarbeitende
• Mitgestaltung bei der Erstellung
• Kontrollaktivitäten ausführen
Eidgenössische Finanzkontrolle:
Prüft regelmässig die IKS in den Verwaltungseinheiten. Die Prüfung des IKS ist Bestandteil der Prüfung der Staatsrechnung

Zentrale Kompetenzstelle und weitere Informationen

Eidgenössische Finanzverwaltung (EFV): Erarbeitet bundesweite Grundlagen und Vorgaben zum Thema Buchführung, Rechnungslegung und IKS und integriert die Themen in Kurse und Ausbildungen.

- Grundlagendokumente: Handbuch für die Haushalt- und Rechnungsführung, Kapitel 4.8

Massnahmenoptionen und Best Practices

- Um die Ordnungsmässigkeit der Buchführung und Rechnungslegung in der Staatsrechnung sicher zu stellen, ist gem. Art. 39 FHG in den Verwaltungseinheiten der zentralen Bundesverwaltung ein wirksames und zweckmässiges Internes Kontrollsystem einzurichten. Die notwendigen Massnahmen sind im IKS-Leitfaden der EFV beschrieben. Dieser ist im Handbuch für die Haushalt- und Rechnungsführung in Kapitel 4.8 abrufbar.

Empfehlungen EFV

Die EFV empfiehlt, im Risikomanagement der Verwaltungseinheit das Risiko der fehlenden Ordnungsmässigkeit in der Buchführung und Rechnungslegung regelmässig zu beurteilen und die Existenz und das dauernde Funktionieren des Internen Kontrollsystems in der Verwaltungseinheit zu prüfen.